



Máster en Ingeniería MultiCloud, DevOps y Seguridad.

AZURE LAB #7

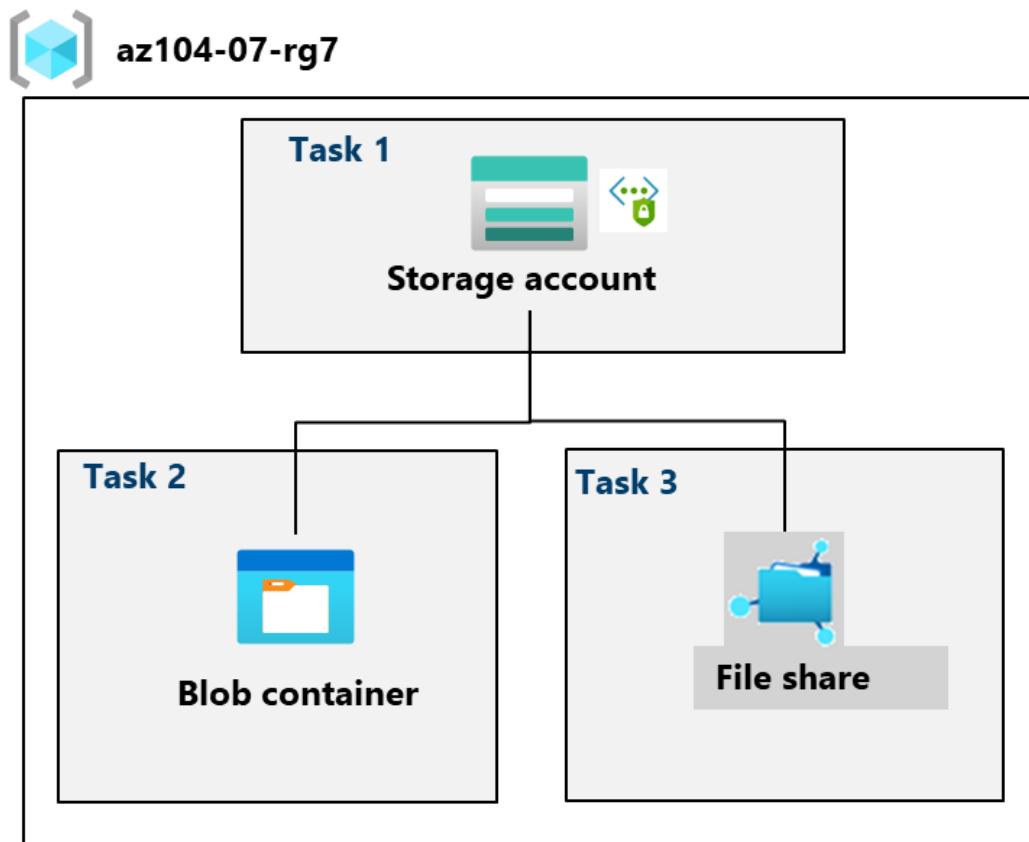
Administración de Azure Storage



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

Esquema del laboratorio





Crear y configurar una cuenta de almacenamiento.

The screenshot shows the 'Create a storage account' wizard in the Azure portal. The 'Basics' tab is selected. The 'Subscription' dropdown is set to 'Azure for Students'. The 'Resource group' dropdown is set to 'az104-rg7' with a 'Create new' link. The 'Storage account name' field contains 'saraul1'. The 'Region' dropdown is set to '(Europe) Germany West Central', which is highlighted with a red box. The 'Preferred storage type' dropdown is set to 'Choose preferred storage type'. A tooltip indicates it helps provide relevant guidance. The 'Performance' section shows 'Standard' (radio button selected) as recommended for most scenarios. The 'Redundancy' section shows 'Geo-redundant storage (GRS)' (dropdown selected) with two optional checkboxes: 'Make read access to data available in the event of regional unavailability.' and 'Geo priority replication guarantees Blob storage data is geo-replicated within 15 minutes.' Both are currently unchecked. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

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.

 tajamar.	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...
<i>Click on add to create a private endpoint</i>						
◀ ▶						

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.



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 ⓘ

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 ⓘ

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 ⓘ

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.



AZURE LAB #7

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

The screenshot shows a deployment summary for 'saraul1_1764924175512'. It includes deployment details like name, subscription, resource group, start time, and correlation ID. It lists three resources: 'saraul1/default' (Microsoft.Storage/storageAccounts/fileservices), 'saraul1/default' (Microsoft.Storage/storageAccounts/blobServices), and 'saraul1' (Microsoft.Storage/storageAccounts). There are sections for 'Deployment details' and 'Next steps' with a 'Go to resource' button.

Creo la cuenta de almacenamiento.

The screenshot shows the 'Public network access' configuration for a storage account. It has two main sections: 'Public network access' and 'Public network access scope'. Under 'Public network access', the 'Enable' option is selected. Under 'Public network access scope', the 'Enable from selected networks' option is selected. In the 'IPv4 Addresses' section, there is a list box containing '95.124.167.181'. The entire 'Public network access' section is highlighted with a red box.

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).



AZURE LAB #7

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

The screenshot shows the Azure Storage account 'saraul1' configuration page. The 'Redundancy' section is selected, showing 'Geo-redundant storage (GRS)' is chosen. Below it, 'Geo priority replication (Blob only)' is disabled. The 'Storage endpoints' table lists two locations:

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

A world map at the bottom shows the locations of the primary and secondary endpoints. The primary endpoint is marked with a blue location pin, and the secondary endpoint is marked with a green location pin.

Miramos donde se estará replicando la cuenta de almacenamiento.



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

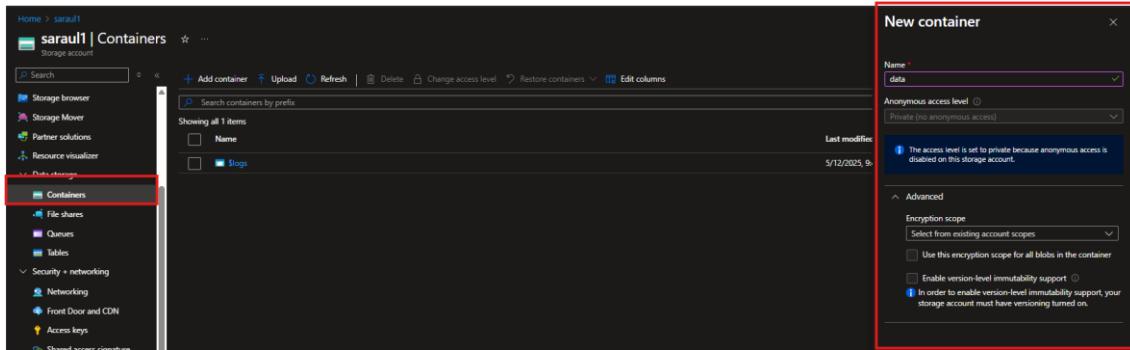
Move to cool storage

+ Add conditions

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

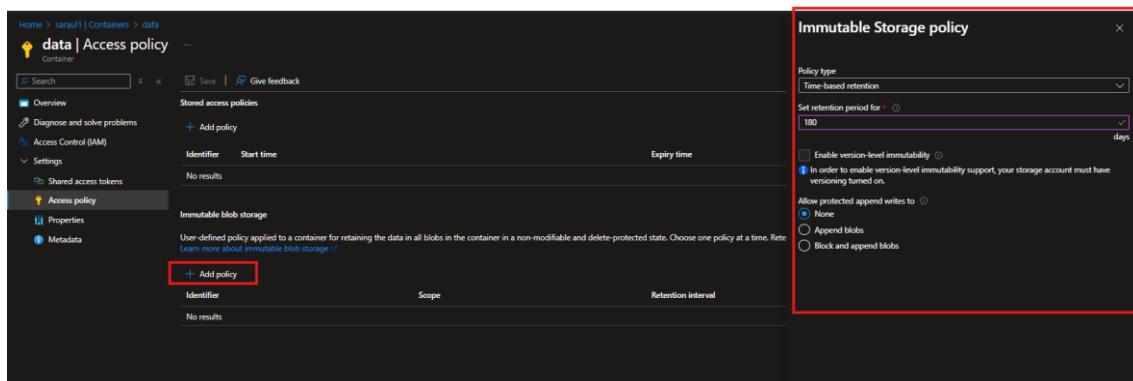
AZURE LAB #7

Creación y configuración del almacenamiento de blobs seguro



The screenshot shows the 'Containers' blade in the Azure Storage account 'saraull1'. A red box highlights the 'Containers' section in the left sidebar. On the right, a 'New container' dialog is open, also with a red border. It shows a 'Name' field with 'data' and an 'Anonymous access level' dropdown set to 'Private (no anonymous access)'. A note at the bottom states: 'The access level is set to private because anonymous access is disabled on this storage account.' Below this, there's an 'Advanced' section with options for 'Encryption scope' (set to 'Select from existing account scopes') and 'Enable version-level immutability support' (unchecked). A note below it says: 'In order to enable version-level immutability support, your storage account must have versioning turned on.'

Dentro de containers creo un nuevo contenedor.



The screenshot shows the 'Access policy' blade for the 'data' container. A red box highlights the 'Access policy' section in the left sidebar. On the right, an 'Immutable Storage policy' dialog is open, also with a red border. It shows a 'Policy type' dropdown set to 'Time-based retention'. Under 'Set retention period for', '180' days is selected. A note below it says: 'In order to enable version-level immutability support, your storage account must have versioning turned on.' At the bottom, there are options for 'Allow protected append writes to': 'None' (radio button selected), 'Append blobs', or 'Block and append blobs'.

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.



AZURE LAB #7

The screenshot shows two windows from the Azure Storage Explorer. The left window displays a container named 'data' with a single folder named 'securitytest'. The right window is an 'Upload blob' dialog where a file named 'AZ-104A 351-400.docx' is being uploaded to the 'securitytest' folder. The 'Upload to folder' field is highlighted with a red box. The resulting list of blobs in the 'data' container shows the uploaded file 'AZ-104A 351-400.docx' with details like Last modified (5/12/2025, 10:16:23), Access tier (Hot (Inferred)), Blob type (Block blob), Size (2.89 MiB), and Lease state (Available).

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.

The screenshot shows a browser window displaying a 403 Forbidden error page. The URL is 'saraul1.blob.core.windows.net/data/securitytest/AZ-104A%20351-400.docx'. The error message states: 'This XML file does not appear to have any style information associated with it. The document tree is shown below.' Below the message is the XML error code: '<Error><Code>PublicAccessNotPermitted</Code><Message>Public access is not permitted on this storage account. RequestId:e5f7b983-401e-0016-71c8-653b36000000 Time:2025-12-05T09:18:59.225025Z</Message></Error>'.

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

 tajamar.	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 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...

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.



AZURE LAB #7



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



AZURE LAB #7

Configuración de Azure file storage.

Home > saraul1 | File shares >
New file share ...

Basics **Backup** **Review + create**

Name *

Performance

Maximum IO/s ⓘ	1000
Maximum capacity	5 TiB
Large file shares	Disabled

To use the SMB protocol with this share, check if you can communicate over port 445. These scripts for [Windows clients](#) and [Linux clients](#) can help. Learn how to [circumvent port 445 issues](#).

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

saraul1 | Storage browser

Storage browser | Help me save costs by tiering unused blobs

File shares

Showing all 1 items

Name	Time	Modified	Quota
share1	Transaction optimized	5/12/2025, 10:28:16	5 TiB

Comprobamos que he creado el file share.

File shares > share1

Authentication method: Access key (Switch to Microsoft Entra user account)

Showing all 1 items

Name	Type	Size
Casado San Andrés_Raúl-lab02a.pdf	File	575.96 KB

Subo un archivo de prueba.



AZURE LAB #7

The screenshot shows the 'Service endpoints' blade for the VNET1 virtual network. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Address space, Connected devices, and Subnets. The main area shows a table with columns: Service, Subnet, Status, and Locations. A red box highlights the '+ Add' button. A modal window titled 'Add service endpoints' is open, with 'Service' dropdown set to 'Microsoft.Storage'. A tooltip at the bottom right of the modal provides information about switching source IP addresses.

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.

The screenshot shows the 'Public network access' configuration for a storage account. It includes sections for 'Public network access', 'Public network access scope', 'Virtual Networks', 'IPv4 Addresses', and 'Resource instances'. A red box highlights the '+ Add a virtual network' button. A modal window titled 'Add networks' is open, with 'Subscription' dropdown set to 'Azure for Students', 'Virtual networks' dropdown set to 'VNET1', and 'Subnets' dropdown set to 'default'. A tooltip at the bottom right of the modal provides information about enabling public network access.

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

Borro mi ip pública de mi equipo.



AZURE LAB #7

The screenshot shows the Azure Storage blade for a user named 'saraull'. On the left, there's a sidebar with 'Favorites', 'Recently viewed', and a 'Blob containers' section containing '\$logs' and 'data'. Below that are 'File shares', 'Queues', and 'Tables'. A large error message 'This request is not authorized to perform this operation.' is centered above a detailed error summary. The summary includes:

Summary	
Session ID: e2ccbc0f5d25433f85c82ff4da1bd105 Extension: Microsoft_Azure_Storage Error code: 403	Resource ID: /subscriptions/e24f79c4-03aa-4981-a9d2-f3c7e44dd... Content: BlobsBlade Storage Request ID: ed0eee60-301e-0023-51cb-655722000000

Details:

- This request is not authorized to perform this operation. RequestId:ed0eee60-301e-0023-51cb-655722000000 Time:2025-12-05T09:43:21.100293Z
- This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address (95.124.167.181) to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. [Learn more](#)

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.