LEARN AZURE · PART 3 · BASICS

# Storage accounts, blobs and access keys

And why your Owner role can't read your own files

VG Viki Gandhi · vikigandhi.com/blog

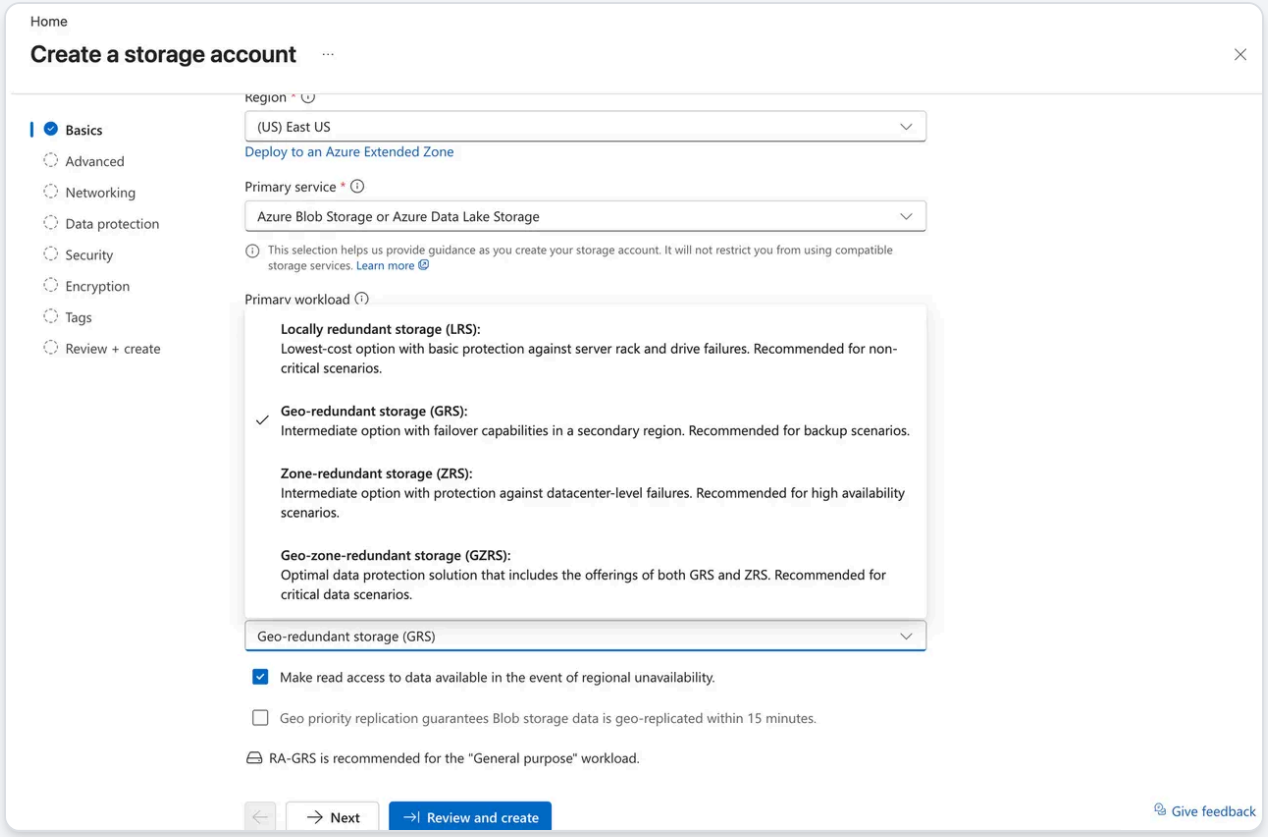
# By the end of this session

- A storage account with sensible, low-cost settings
- A private container with a file in it
- A time-limited SAS link, then broken on purpose
- Data access through your own sign-in, with no key

# One account, four kinds of storage

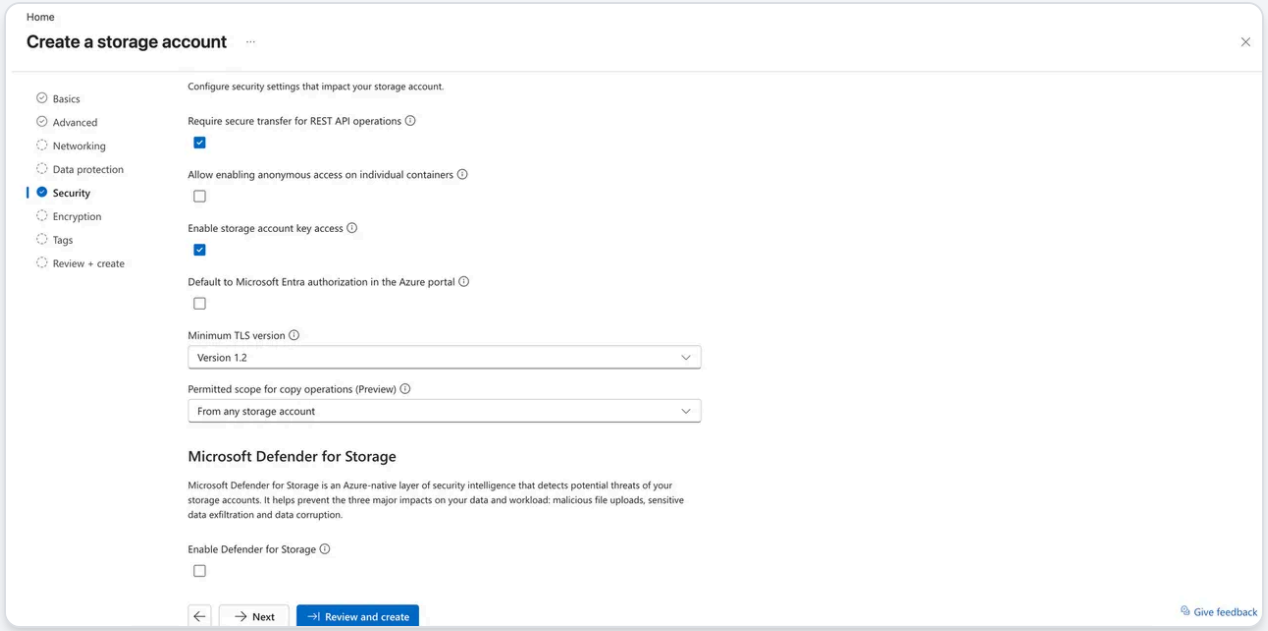
| | | |
|---|---|---|
| **Blobs** | Files of any kind | *Images, backups, documents* |
| **Files** | Network file shares | *Replacing a file server* |
| **Queues** | Small messages | *Passing work between app parts* |
| **Tables** | Key-value rows | *Cheap schema-less data* |

# Redundancy: the setting that doubles your bill



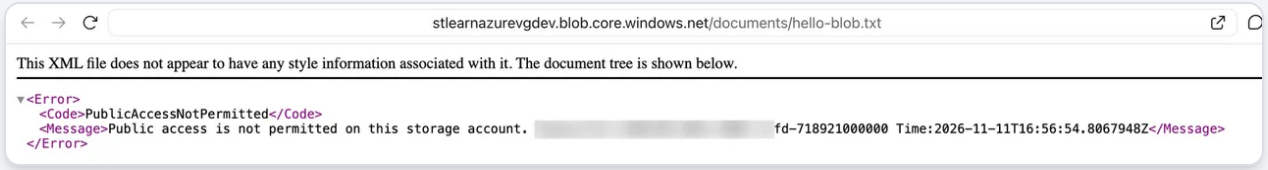

- Default for General purpose: RA-GRS
- LRS: 3 copies, one datacenter, lowest cost
- Geo-redundant: 6 copies, two regions, about double

# Security defaults to notice



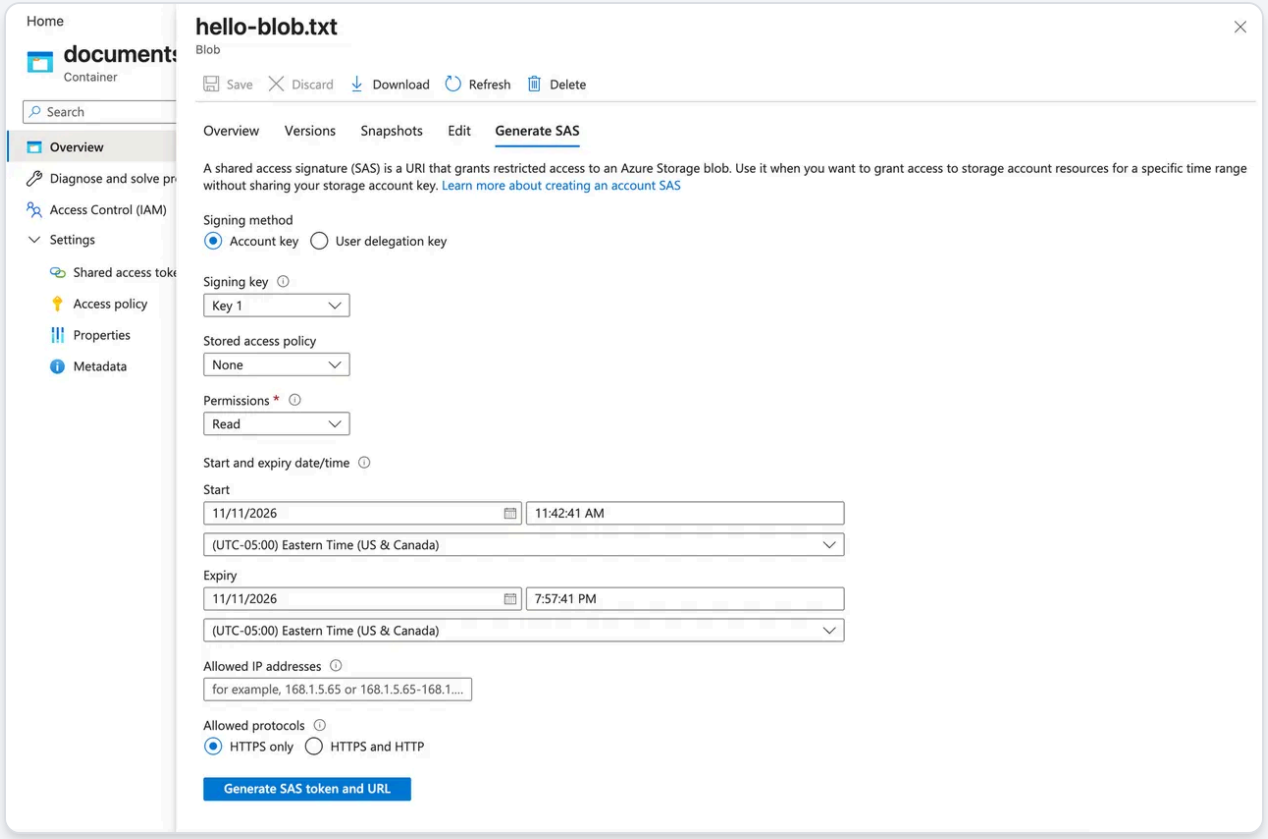

- Anonymous access: off
- Storage account key access: on
- Defender for Storage: off (paid add-on)

# Way 1: open the URL




- PublicAccessNotPermitted
- The URL is public, the data is not

# Way 2: a SAS link



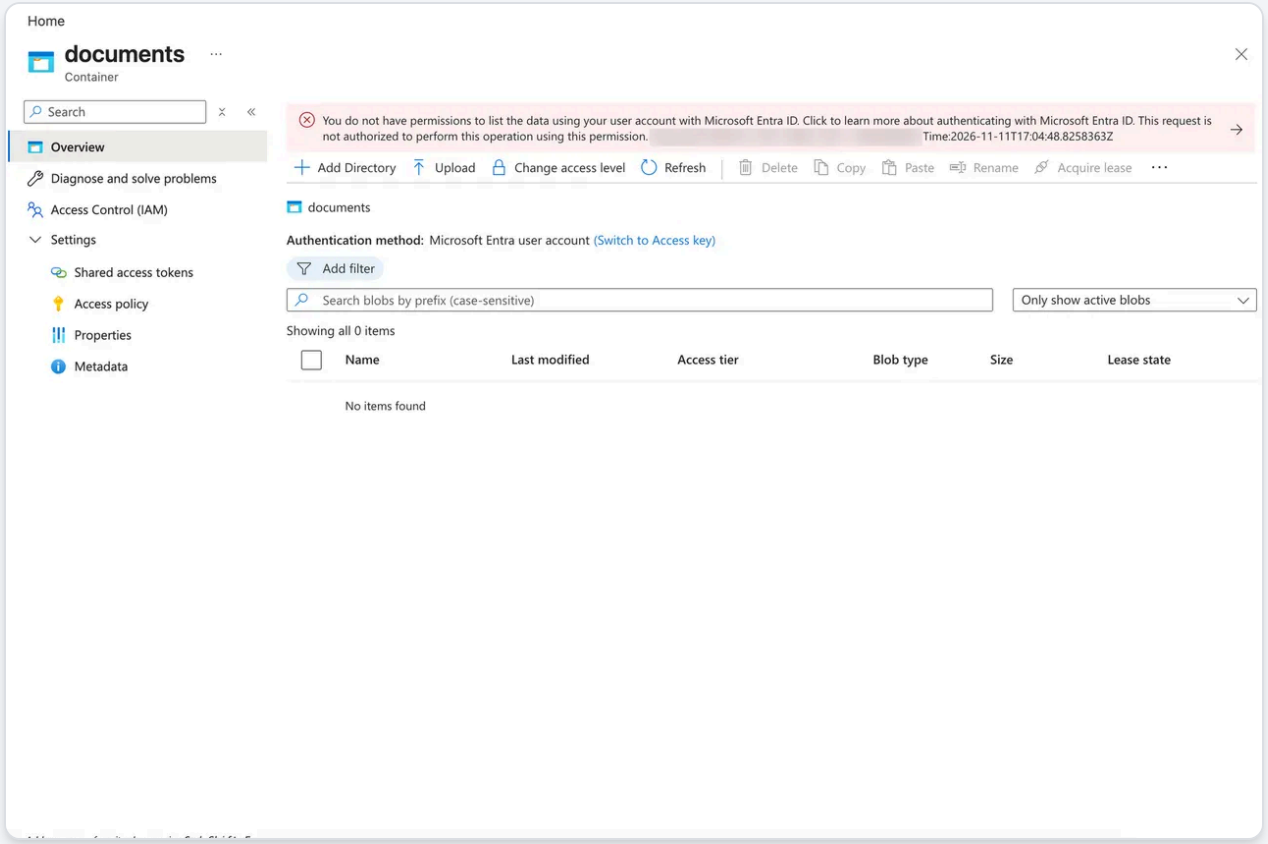

- Read only, one file, HTTPS only
- Expires in hours
- Signed with an account key

REMEMBER

# An account key is a master password

Full read, write and delete on all data, never expires, not tied to a person. Rotating key1 instantly broke our SAS link, and would break every app using it.

# Way 3: sign in as yourself

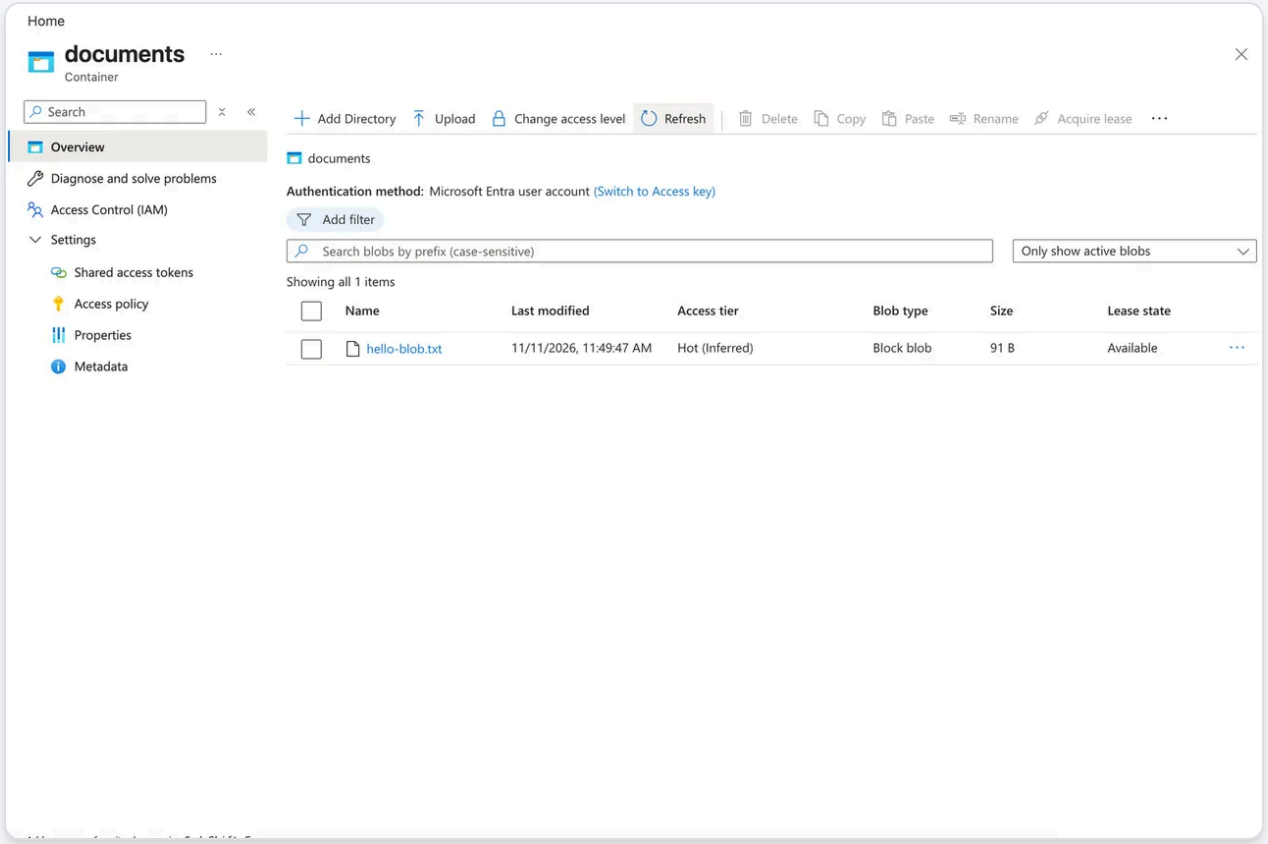



- Owner still gets "no permission to list the data"
- Owner manages resources
- Reading data needs a data role

# Two kinds of permission

| | | |
|---|---|---|
| **Management** | Create, configure, delete resources | *Owner, Contributor, Reader* |
| **Data** | Read and write the contents | *Storage Blob Data Reader / Contributor / Owner* |

# The right way




- Storage Blob Data Contributor, scoped to one account
- Took about 90 seconds to apply
- Logged per person, revocable per person

REMEMBER

# Rule of thumb

Entra roles by default. A short-lived user delegation SAS for outsiders. Account keys only in an emergency, and turn them off once nothing needs them.

# Quick check

- When is LRS a better choice than RA-GRS?
- You rotate key1. What happens to SAS links signed with it?
- Why can't the subscription Owner list blobs with Entra sign-in?
- Why is an account key riskier than a role assignment?

Answers are in the post.

UP NEXT

# Next: reading your bill before it surprises you

Open Cost analysis, find what the last three posts actually cost, and build views that make surprises easy to spot.