

Azure Identity, Access, and Storage Management

Project Overview

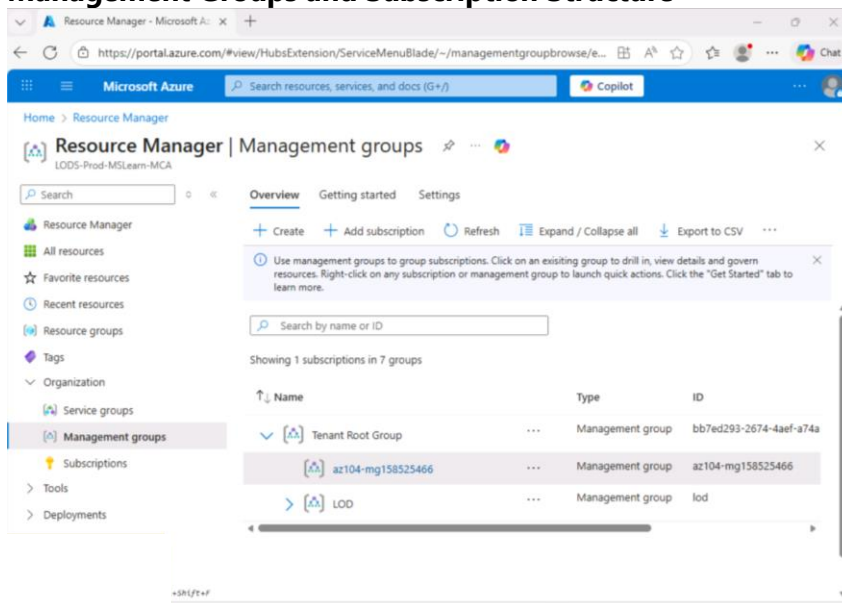
This document summarizes hands-on experience managing Azure identity and access controls, subscription governance, and secure storage services using the Azure Portal.

- Implemented governance, access control, and secure storage best practices

Subscription Governance and Role-Based Access Control (RBAC)

This section documents the management of Azure subscriptions and access control using management groups and role-based access control (RBAC), including role assignment, custom role creation, and monitoring access changes through audit logs.

Management Groups and Subscription Structure



The screenshot shows the Microsoft Azure portal interface. At the top, the breadcrumb navigation indicates the path: Home > Resource Manager | Management groups > az104-mg158525466. The main heading is 'az104-mg158525466 | Access control (IAM)'. The left-hand navigation pane lists several options: Overview, Subscriptions, Resource Groups, Resources, Activity Log, Access control (IAM) (which is selected), Governance, and Cost Management. The main content area is titled 'Check access' and has a sub-tab 'Role assignments'. Below this, there is a search bar containing 'IT'. The search results are filtered by 'Type: All', 'Role: All', 'Scope: All scopes', 'State: All', and 'End time: All'. The results are grouped by 'Role'. Under the 'All (1)' group, there is a table of role assignments. The table has columns for Name, Type, Role, and Scope. One assignment is listed: 'IT Helpdesk' (Name), 'ef10b83c-567d...' (ID), 'Virtual Machine Contributor' (Role), and 'This resource' (Scope). At the bottom, it says 'Showing 1 - 1 of 1 results.' The bottom right corner shows the date and time: 'Friday, January 23, 2020' and 'Fri 8:21 AM (Local time)'.

Home > Resource Manager | Management groups > az104-mg158525466

az104-mg158525466 | Access control (IAM)

Management group

Search

Add Download role assignments Edit columns Refresh Delete Feedback

Overview

Subscriptions

Resource Groups

Resources

Activity Log

Access control (IAM)

Governance

Cost Management

Check access

Role assignments Roles Deny assignments

IT

Type: All Role: All Scope: All scopes State: All End time: All

Group by: Role

All (1) Job function roles (1) Privileged administrator roles (0)

Name	Type	Role	Scope
IT Helpdesk ef10b83c-567d...	Group	Virtual Machine Contributor	This resource

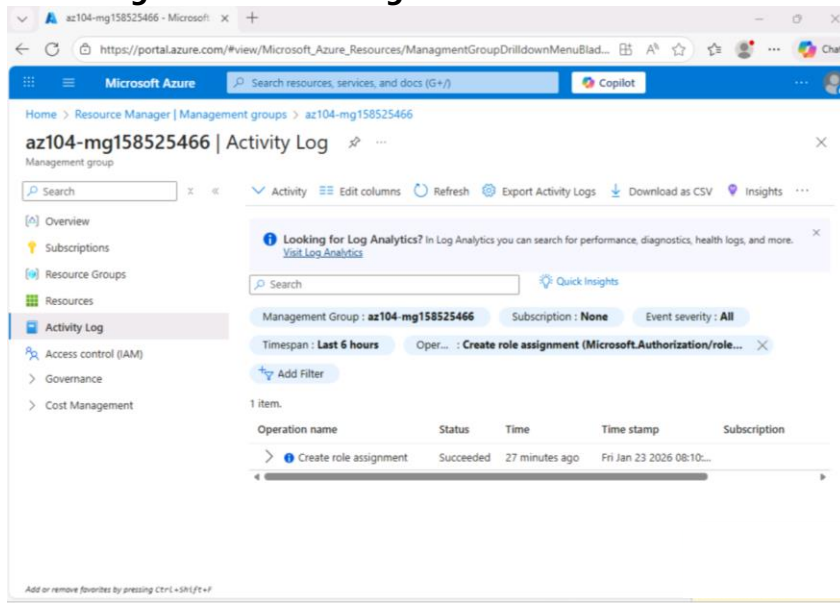
Showing 1 - 1 of 1 results.

Friday, January 23, 2020

Fri 8:21 AM (Local time)

[illegible]

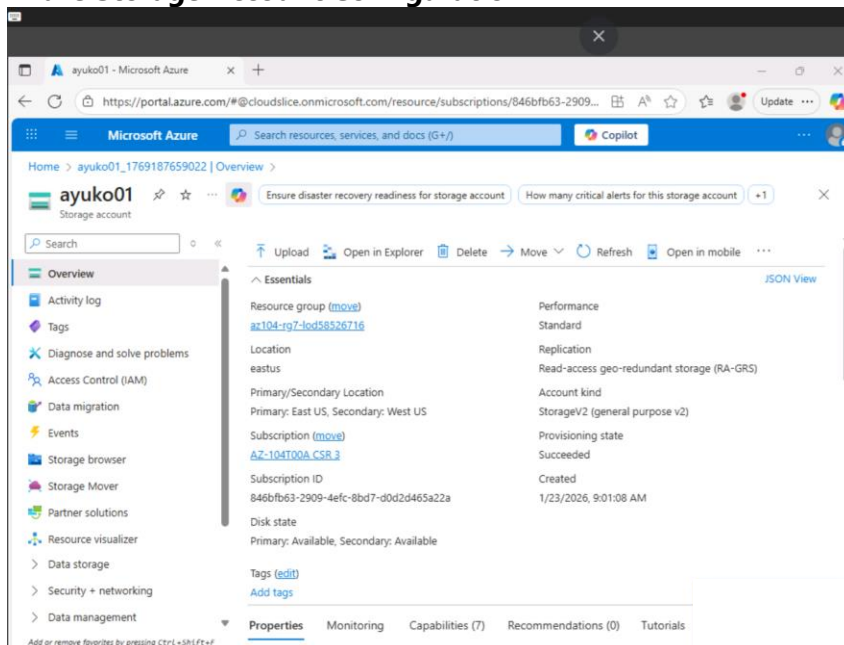
Role Assignment Monitoring



Secure Azure Storage Configuration

This section documents the configuration of Azure Storage services with a focus on security, access control, and network restrictions, including Blob and File storage setup and data access management.

Azure Storage Account Configuration



ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...

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

Home > ayuko01_1769187659022 | Overview >

ayuko01 Storage account

Ensure disaster recovery readiness for storage account How many critical alerts for this storage account +1

Search

Overview

- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Storage Mover
- Partner solutions
- Resource visualizer
- Data storage
- Security + networking
- Data management

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service

- Hierarchical namespace Disabled
- Default access tier Hot
- Blob anonymous access Disabled
- Blob soft delete Enabled (7 days)
- Container soft delete Enabled (7 days)
- Versioning Disabled
- Change feed Disabled
- NFS v3 Disabled
- Allow cross-tenant replication Disabled
- Storage tasks assignments None

Security

- Require secure transfer for REST API operations Enabled
- Storage account key access Enabled
- Minimum TLS version Version 1.2
- Infrastructure encryption Disabled

Networking

- Public network access Disabled
- Private endpoint connections 0
- Network routing Microsoft network routing
- Endpoint type Standard

Add or remove favorites by pressing Ctrl+Shift+F

ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...

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

Home > ayuko01_1769187659022 | Overview > ayuko01

ayuko01 Storage account

Search

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Security + networking

Networking

- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for

Public access Private endpoints Network routing Custom domain

Configure access to this storage account using Virtual Networks, IP address ranges, or a network security perimeter. [Learn more](#)

Associate a network security perimeter to secure public network access. [View recommendations](#)

Public network access Enabled from selected networks

Manage

Network security perimeter

Associate a network security perimeter to centrally manage inbound and outbound access rules. [Learn more](#)

No network security perimeter has been associated

Associate

Resource settings: Virtual networks, IP addresses, and exceptions

Configure access rules to specify which networks can access this storage account. [Learn more](#)

Access rules None

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure

Home > ayuko01_1769187659022 | Overview > ayuko01 | Lifecycle management >

Add a rule

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

Previous

Add

ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...

Microsoft Azure

Home > ayuko01_1769187659022 | Overview > ayuko01

ayuko01 | Lifecycle management

Storage account

Search

+ Add a rule ✓ Enable ☐ Disable ☐ Refresh Delete Give feedback

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

Add or remove favorites by pressing Ctrl+L+Shift+F

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle. A new or updated rule can take up to 24 hours to go into effect. [Learn more](#)

List View Code View

Enable access tracking ☐

Name	Status	Blob type
Movetocool	Enabled	Block

Secure Blob Storage and Retention Policies

- Blob Container Creation and Retention Policy Configuration

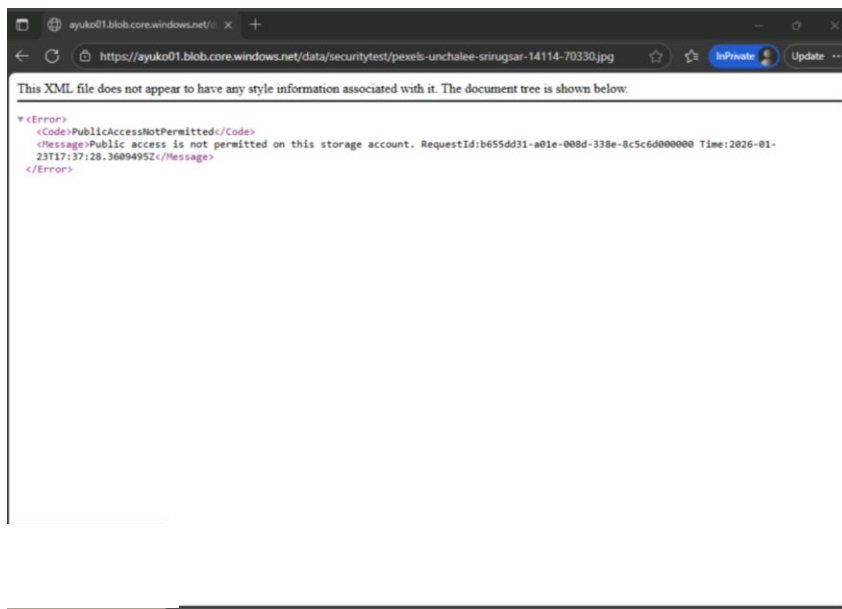
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Containers' section under 'Data storage'. The main area displays the 'Access policy' configuration for a container named 'data'. The 'Stored access policies' section is empty, with a '+ Add policy' button. Below this, the 'Immutable blob storage' section is visible, showing a table with columns: Identifier, Scope, Retention interval, and State. The table contains one entry: 'Time-based retention' for the 'Container' scope, with a retention interval of '180 days' and a state of 'Unlocked'.

Identifier	Scope	Retention interval	State
Time-based retention	Container	180 days	Unlocked

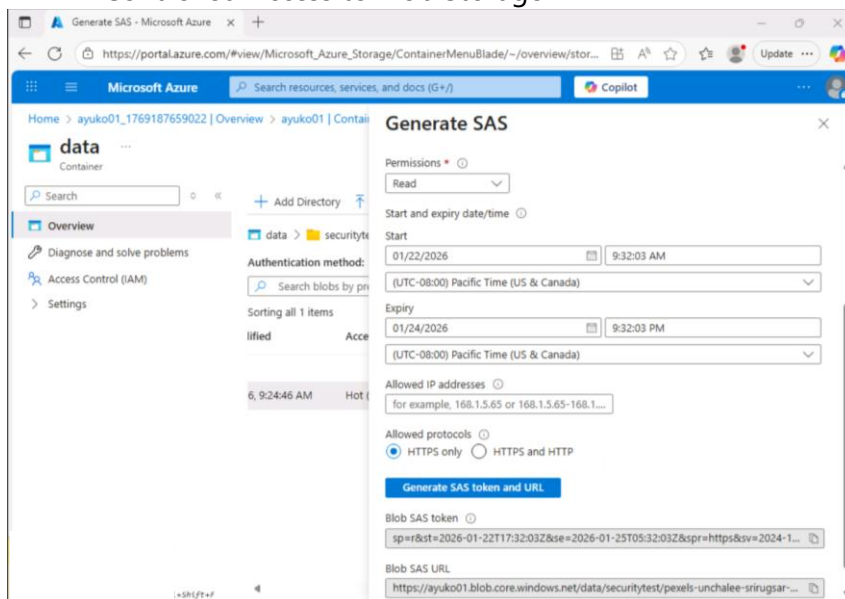
- Blob Upload and Management

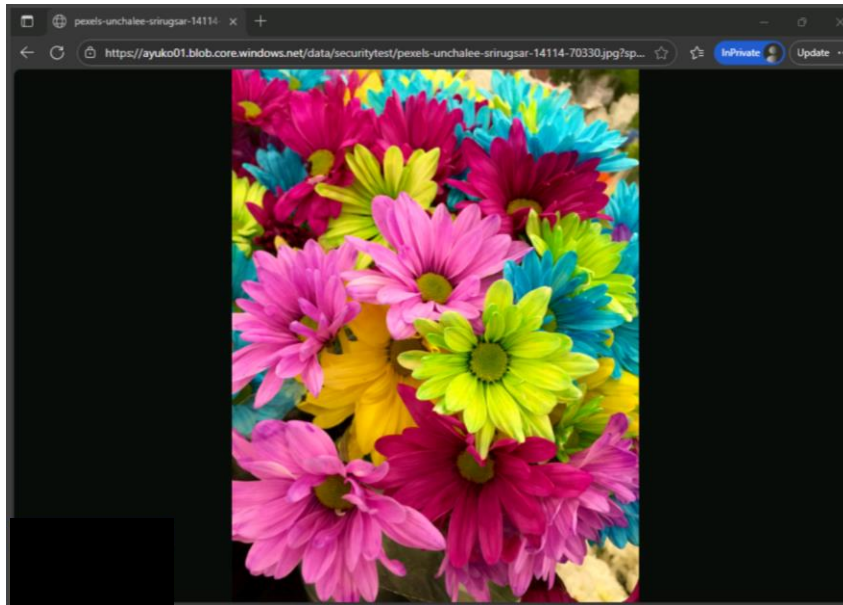
The screenshot shows the Microsoft Azure portal interface for a container named 'data'. The 'Overview' tab is selected, showing a list of blobs. The 'Authentication method' is set to 'Access key'. The 'Showing all 1 items' section displays a table with columns: Name, Last modified, Access tier, Blob type, and Size. The table contains one entry: 'pesels-unc...' with a last modified date of '1/23/2026, 9:24:46 AM', an access tier of 'Hot (Inferred)', a blob type of 'Block blob', and a size of '722.94'.

Name	Last modified	Access tier	Blob type	Size
pesels-unc...	1/23/2026, 9:24:46 AM	Hot (Inferred)	Block blob	722.94

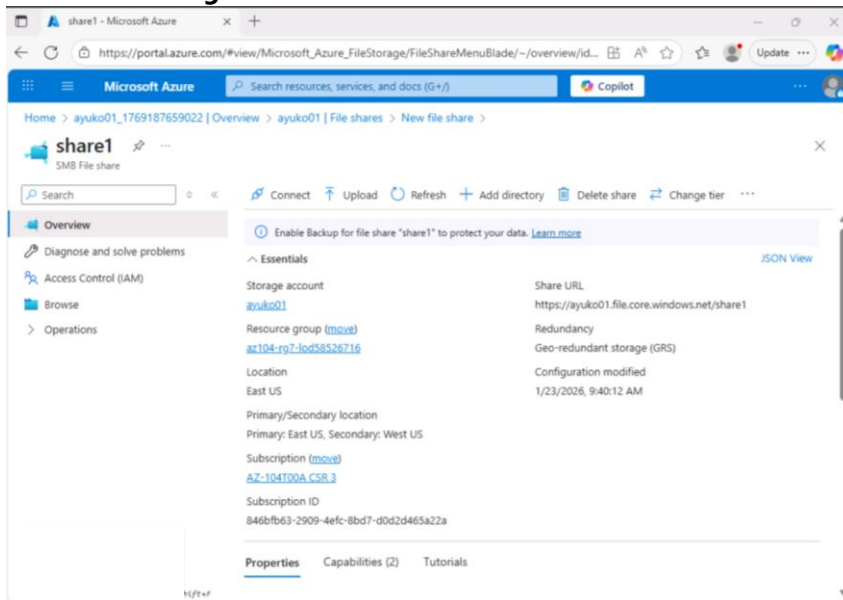


- Controlled Access to Blob Storage

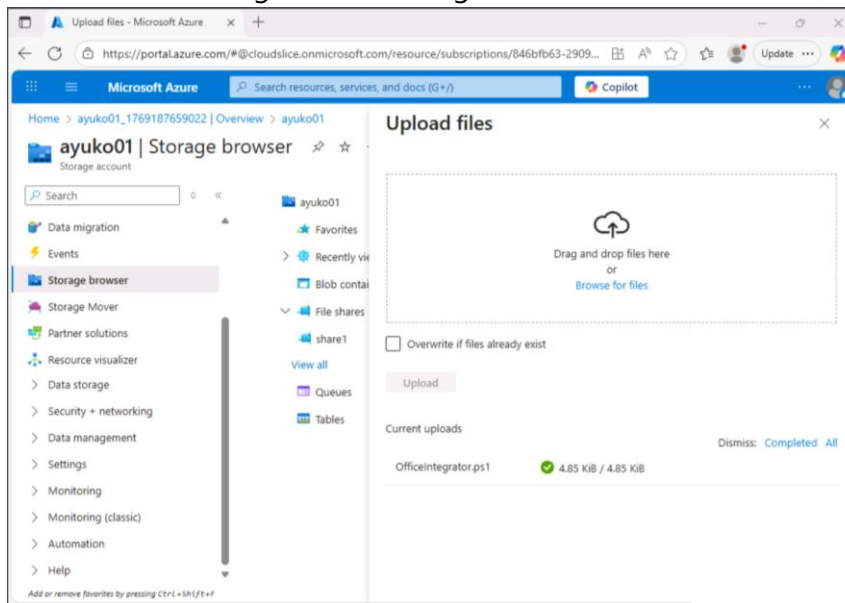




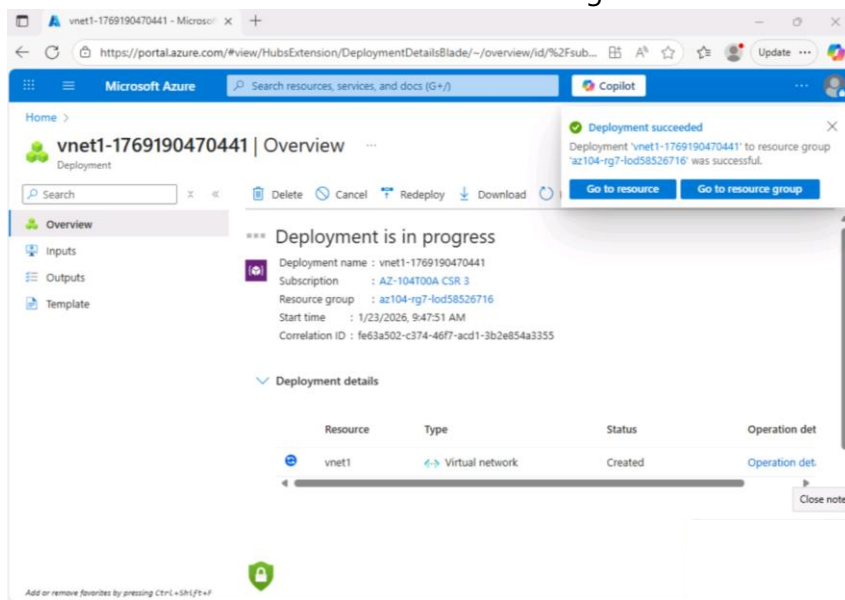
Azure File Storage and Network Restrictions



- Azure Storage Browser Usage



- Network Access Restrictions for Storage Accounts



Microsoft Azure | vnet1-1769190470441 | Overview > vnet1

vnet1 | Service endpoints

Virtual network

Search + Add Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
 - Address space
 - Connected devices
 - Subnets
 - Bastion
 - DDoS protection
 - Firewall
 - Microsoft Defender for Cloud

Filter service endpoints

Service	Subnet	Status	Locations
Microsoft.Storage	1	Succeeded	East US, West US, West US 3

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure | ayuko01 | Networking >

Public network access

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
> vnet1	1	10.0.0.0/16		az104-rg7-lod5...	AZ-104T00A CS...

IPv4 Addresses

Allow select public internet IP addresses to access your resource. [Learn more](#)

+ Add your client IPv4 address ("168.245.203.246")

IPv4 address or CIDR

Resource instances

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

ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...

Microsoft Azure

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

Copilot

Home > ayuko01

ayuko01 | Networking

Storage account

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Add or remove favorites by pressing Ctrl+L+Sh/⌘+F

Learn more

Associate a network security perimeter to secure public network access. [View recommendations](#)

Public network access Enabled from selected networks

Manage

Network security perimeter

Associate a network security perimeter to centrally manage inbound and outbound access rules. [Learn more](#)

No network security perimeter has been associated

Associate

Resource settings: Virtual networks, IP addresses, and exceptions

Configure access rules to specify which networks can access this storage account. [Learn more](#)

Access rules	None
Virtual networks	1
IPv4 addresses	None
Exceptions	1

ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...

Microsoft Azure

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

Copilot

Home > ayuko01

ayuko01 | Storage browser

Storage account

Help me save costs by tiering unused blobs

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

ayuko01

Favorites

Recently viewed

Blob containers

File shares

share1

View all

Queues

Tables

This request is not authorized to perform this operation.

Summary

Session ID
6055d313409a4ad4b39383819211c848

Resource ID
/subscriptions/846bfb63-2909-4efc-8...

Extension
Microsoft_Azure_Storage

Content
FilesBlade

Error code
403

Storage Request ID
98114c8b-201a-009f-3691-8c27bd00...