

Azure Identity, Access, and Storage Management

Project Overview

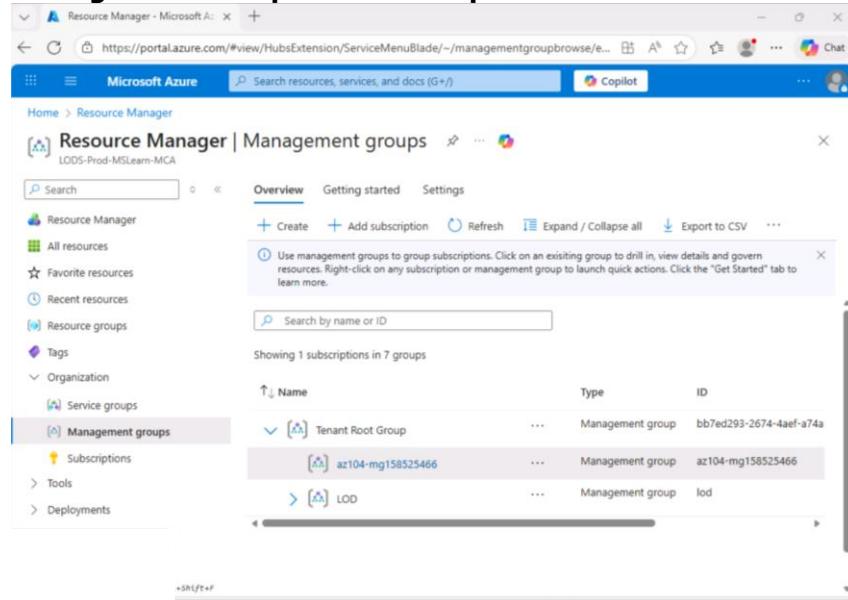
This document summarizes hands-on experience managing Azure identity and access controls, subscription governance, and secure storage services using the Azure Portal.

- 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 Azure Resource Manager - Management groups interface. The left sidebar lists navigation options: Home, Resource Manager, All resources, Favorite resources, Recent resources, Resource groups, Tags, Organization, Service groups, Management groups (which is selected and highlighted in blue), Subscriptions, Tools, and Deployments. The main content area has tabs for Overview, Getting started, and Settings, with Overview selected. It displays a table of subscriptions grouped by management groups. A search bar at the top allows searching by name or ID. A tooltip provides information about management groups. The table data is as follows:

| Name | Type | ID |
|-------------------|------------------|-------------------------|
| Tenant Root Group | Management group | bb7ed293-2674-4aef-a74a |
| az104-mg158525466 | Management group | az104-mg158525466 |
| LOD | Management group | lod |

Built-in and Custom RBAC Roles

The screenshot shows the Microsoft Azure portal interface. The URL is https://portal.azure.com/#view/Microsoft_Azure_Resources/ManagementGroupDrilldownMenuBlade/az104-mg158525466. The page title is "az104-mg158525466 | Access control (IAM)". The left sidebar shows "Access control (IAM)" selected under "Management group". The main content area has tabs: "Role assignments" (selected), "Check access", "Roles", and "Deny assignments". A search bar at the top says "P IT". Below it are filters: Type: All, Role: All, Scope: All scopes, State: All, End time: All, and Group by: Role. The results table shows one entry: "Virtual Machine Contributor" (Group) assigned to "IT Helpdesk" (Group). The table has columns: Name, Type, Role, and Scope. At the bottom, it says "Showing 1 - 1 of 1 results." The footer shows the date "Friday, January 23, 2026" and time "Fri 8:21 AM (Local time)".

The screenshot shows the Microsoft Azure portal interface. The URL is https://portal.azure.com/#view/Microsoft_Azure_AD/CreateCustomRoleLandingBlade/roleId-/null. The page title is "Create a custom role". The message box says: "You have successfully created the custom role "Custom Support Request58525466". It may take the system a few minutes to display your role everywhere." There is an "OK" button. Below it, the "Role description" is "A custom contributor role for support requests.". The "Permissions" section lists actions: Action: Microsoft.Authorization/*/read, Action: Microsoft.Resources/subscriptions/resourceGroups/read, Action: Microsoft.Support/*, NotAction: Microsoft.Support/register/action. The "Assignable Scopes" section shows a scope: "/providers/Microsoft.Management/managementGroups/az104-mg158525466". At the bottom are "Create" and "Previous" buttons.

Role Assignment Monitoring

The screenshot shows the Microsoft Azure Activity Log page for the management group 'az104-mg158525466'. The left sidebar lists 'Activity Log' as the selected item under 'Management group'. The main area displays a single log entry:

| Operation name | Status | Time | Time stamp | Subscription |
|------------------------|-----------|----------------|--------------------------|--------------|
| Create role assignment | Succeeded | 27 minutes ago | Fri Jan 23 2026 08:10... | |

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

The screenshot shows the Microsoft Azure Storage account configuration page for 'ayuko01'. The left sidebar shows various options like Overview, Activity log, Tags, and Diagnose and solve problems. The main pane displays the account's properties:

| Resource group (move) | Performance |
|--|--|
| az104-rg7-lod58526716 | Standard |
| Location | Replication |
| eastus | Read-access geo-redundant storage (RA-GRS) |
| Primary/Secondary Location | Account kind |
| Primary: East US, Secondary: West US | StorageV2 (general purpose v2) |
| Subscription (move) | Provisioning state |
| AZ-104T00A.CSR.2 | Succeeded |
| Subscription ID | Created |
| 846fbf63-2909-4efc-8bd7-d0d2d465a22a | 1/23/2026, 9:01:08 AM |
| Disk state | |
| Primary: Available, Secondary: Available | |

ayuko01 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846fbfb63-2909...

Microsoft Azure

ayuko01 | Overview

Storage account

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

Overview

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

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/846fbfb63-2909...

Microsoft Azure

ayuko01 | Overview > ayuko01

Storage account

Search

Public access Private endpoints Network routing Custom domain

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

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**

Add a rule - Microsoft Azure

https://portal.azure.com/#view/Microsoft_Azure_Storage/AddRuleView.ReactView/storageAccount

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

Copilot

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 Search resources, services, and docs (G+)

Copilot

Home > ayuko01_1769187659022 | Overview > ayuko01

ayuko01 | Lifecycle management

Storage account

+ Add a rule ✓ Enable □ Disable ⏪ Refresh ⏺ Delete ⏹ Give feedback

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 |

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+Shift+F**

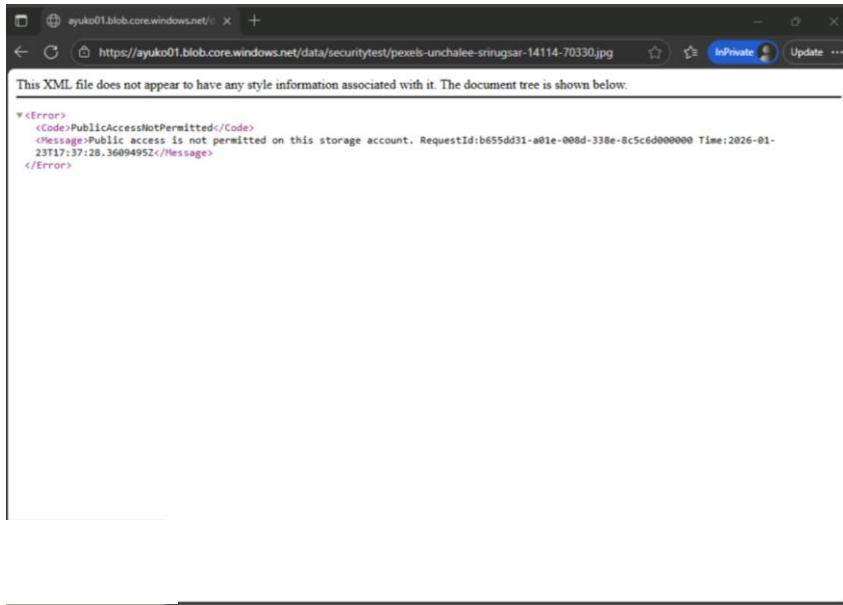
Secure Blob Storage and Retention Policies

- Blob Container Creation and Retention Policy Configuration

The screenshot shows the Microsoft Azure portal interface for managing access policies. The left sidebar is for the storage account 'ayuko01'. The main area is titled 'Access policy' under 'data'. It shows a table for 'Stored access policies' with columns: Identifier, Start time, Expiry time, and Permissions. A note says 'No results'. Below this is a section for 'Immutable blob storage' with a note about user-defined policies for retaining data. A table for 'Time-based retention' shows a single row: 'Time-based retention' (Identifier), 'Container' (Scope), '180 days' (Retention interval), and 'Unlocked' (State). There are buttons for '+ Add policy'.

- Blob Upload and Management

The screenshot shows the Microsoft Azure portal interface for managing blobs within a container named 'data'. The left sidebar is for the storage account 'ayuko01'. The main area shows a list of blobs. At the top, there are buttons for '+ Add Directory', 'Upload', 'Refresh', 'Delete', 'Copy', 'Paste', 'Rename', and '...'. A search bar and a dropdown menu 'Only show active blobs' are also present. The list table has columns: Name, Last modified, Access tier, Blob type, and Size. One blob is selected, showing details: 'pixels-unc...' (Name), '1/23/2026, 9:24:46 AM' (Last modified), 'Hot (Inferred)' (Access tier), 'Block blob' (Blob type), and '722.94' (Size).



- Controlled Access to Blob Storage

The screenshot shows the Microsoft Azure portal interface for generating a Shared Access Signature (SAS) token. The URL in the address bar is https://portal.azure.com/#view/Microsoft_Azure_Storage/ContainerMenuBlade/~/overview/storageAccounts/ayuko01.

Generate SAS

Permissions: Read

Start and expiry date/time:

- Start: 01/22/2026, 9:32:03 AM (UTC-08:00) Pacific Time (US & Canada)
- Expiry: 01/24/2026, 9:32:03 PM (UTC-08:00) Pacific Time (US & Canada)

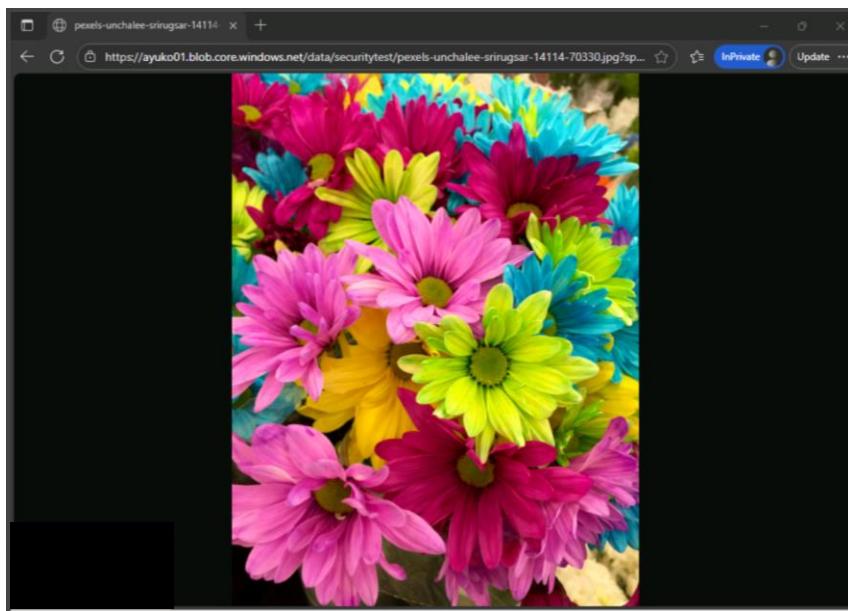
Allowed IP addresses: (example, 168.1.5.65 or 168.1.5.65-168.1...)

Allowed protocols: HTTPS only HTTPS and HTTP

Generate SAS token and URL:

Blob SAS token: `sp=r&t=2026-01-22T17:32:03Z&se=2026-01-25T05:32:03Z&spr=https&sv=2024-1...`

Blob SAS URL: <https://ayuko01.blob.core.windows.net/data/securitytest/pexels-unchalee-sirurgsar-14114-70330.jpg>



Azure File Storage and Network Restrictions

A screenshot of the Microsoft Azure portal. The left sidebar shows a navigation tree with "Home", "ayuko01_1769187659022", "Overview", "ayuko01", "File shares", and "New file share >". The main content area is titled "share1" and "SMB File share". It features a "Search" bar and a toolbar with "Connect", "Upload", "Refresh", "Add directory", "Delete share", "Change tier", and more. On the left, there's a "Overview" section with a "Diagnose and solve problems" button, "Access Control (IAM)", "Browse", and "Operations". The "Essentials" section provides details: Storage account "ayuko01", Share URL "https://ayuko01.file.core.windows.net/share1", Resource group "az104-rg7-lod58526716", Redundancy "Geo-redundant storage (GRS)", Location "East US", Configuration "modified", and Last modified "1/23/2026, 9:40:12 AM". A "Subscription" section lists "AZ-104T00A_CSR_3" and "Subscription ID 846fb63-2909-4efc-8bd7-d0d2d465a22a". At the bottom, there are "Properties", "Capabilities (2)", and "Tutorials" buttons.

- Azure Storage Browser Usage

The screenshot shows the Microsoft Azure Storage browser interface. On the left, there is a sidebar with various options like Data migration, Events, Storage Mover, Partner solutions, Resource visualizer, and Storage browser (which is currently selected). The main area is titled "Upload files" and contains a large dashed box with a cloud icon and the text "Drag and drop files here or Browse for files". Below this, there is a checkbox for "Overwrite if files already exist" and a "Upload" button. Under "Current uploads", there is a file named "Officeintegrator.pst" with a size of "4.85 KB / 4.85 KB". At the bottom right, there are buttons for "Dismiss", "Completed", and "All".

- Network Access Restrictions for Storage Accounts

The screenshot shows the Microsoft Azure Overview page for a virtual network named "vnet1-1769190470441". The top right corner displays a green checkmark icon and the text "Deployment succeeded". The main area is titled "Deployment is in progress" and provides details about the deployment: Deployment name: vnet1-1769190470441, Subscription: AZ-104700A CSR 3, Resource group: az104-rg7-lod58526716, Start time: 1/23/2026, 9:47:51 AM, Correlation ID: fe63a502-c374-46f7-acd1-3b2e854a3355. Below this, there is a section titled "Deployment details" which lists a single resource: "vnet1" (Type: Virtual network, Status: Created). A note at the bottom right says "Close note".

vnet1 - Microsoft Azure

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846fb63-2909...

Microsoft Azure

Home > 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

Add or remove favorites by pressing Ctrl+Shift+F

Service Subnet Status Locations

Microsoft.Storage 1 Succeeded East US, West US, West US 3

Public network access - Microsoft

https://portal.azure.com/#view/Microsoft_Azure_Storage/ConfigurePublicNetworkAccessAndRes...

Microsoft Azure

Home > 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 | Succeeded | az104-rg7-lod5... | AZ-104T00A CS:u... |

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](#)

Save Cancel

ayuko01 - Microsoft Azure

Home > ayuko01

ayuko01 | Networking

Storage account

Search

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

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

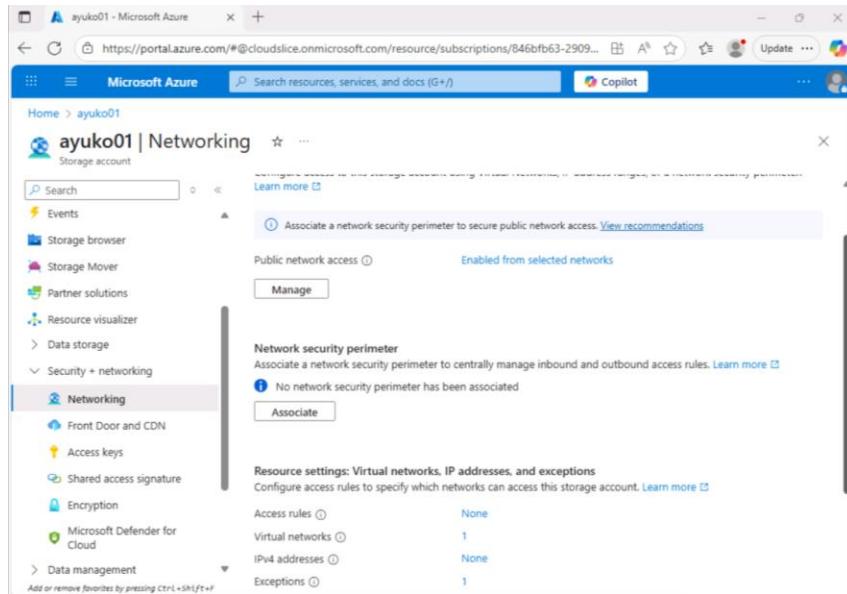
Associate

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 |

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



ayuko01 - Microsoft Azure

Home > ayuko01

ayuko01 | Storage browser

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Favorites

Recently viewed

Blob containers

File shares

share1

View all

Queues

Tables

Help me save costs by tiering unused blobs

This request is not authorized to perform this operation.

Summary

| Session ID | 6055d313409a4ad4b39383819211c648 |
|--------------------|---------------------------------------|
| Resource ID | /subscriptions/846fb63-2909-4efc-8... |
| Extension | Microsoft_Azure_Storage |
| Content | FileBlade |
| Error code | 403 |
| Storage Request ID | 98114c8b-301a-009f-3691-8c27bd00... |

