

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 - Microsoft Azure portal. On the left, the 'Management groups' blade is open, displaying a list of existing management groups: Tenant Root Group, az104-mg158525466, and LOD. The 'az104-mg158525466' group is currently selected. On the right, a 'Manage Subscriptions and RBAC' blade is open, providing step-by-step instructions for creating a new management group. The steps are:

5. Search for and select Management groups.
6. On the Management groups blade, click + Create.
7. Create a management group with the following settings. Select Submit when you are done.

Setting	Value
Management group ID	az104-mg158525466 (must be unique in the directory)
Management group display name	az104-mg158525466
8. Refresh the management group page to ensure your new management group displays. This may take a minute.

Note: Did you notice the root management group? The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level. After creating a management group, you would add any subscriptions that should be included in the group.

Built-in and Custom RBAC Roles

Instructions **Resources**

Did you know? Azure originally provided only the **Classic** deployment model. This has been replaced by the **Azure Resource Manager** deployment model. As a best practice, do not use classic resources.

6. On the **Members** tab, Select **Members**.
7. Search for and select the **IT Helpdesk** group. Click **Select**.
8. Click **Review + assign** twice to create the role assignment.
9. Continue on the **Access control (IAM)** blade. On the **Role assignments** tab, confirm the **IT Helpdesk** group has the **Virtual Machine Contributor** role.

Note: As a best practice always assign roles to groups not individuals.

Did you know? This assignment might not actually grant you any additional privileges. If you already have the **Owner** role, that role includes all permissions associated with the VM Contributor role.

41 Minutes Remaining

Role Assignment Monitoring

Instructions **Resources**

should be updated to include this permission as a *NotAction*.

Note: An Azure resource provider is a set of REST operations that enable functionality for a specific Azure service. We do not want the Help Desk to be able to have this capability, so it is being removed from the cloned role.

8. On the **Assignable scopes** tab, ensure your management group is listed, then click **Next**.
9. Review the JSON for the **Actions**, **NotActions**, and **AssignableScopes** that are customized in the role.
10. Select **Review + Create**, and then select **Create**.

Note: At this point, you have created a custom role and assigned it to the management group.

Task 4: Monitor role assignments with the Activity Log

32 Minutes Remaining

Instructions Resources

- 9. Review the JSON for the *Actions*, *NotActions*, and *AssignableScopes* that are customized in the role.
- 10. Select **Review + Create**, and then select **Create**.

Note: At this point, you have created a custom role and assigned it to the management group.

Task 4: Monitor role assignments with the Activity Log

In this task, you view the activity log to determine if anyone has created a new role.

1. In the portal locate the **az104-mg158525466** resource and select **Activity log**. The activity log provides insight into subscription-level events.
2. Review the activities for role assignments. The activity log can be filtered for specific operations.

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

Instructions Resources

- 5. On the **Networking** tab, in the **Public network access** section, select **Disable**. This will restrict inbound access while allowing outbound access.
- 6. Review the **Data protection** tab. Notice 7 days is the default soft delete retention policy. Note you can enable versioning for blobs. Accept the defaults.
- 7. Review the **Encryption** tab. Notice the additional security options. Accept the defaults.
- 8. Select **Review + create**, wait for the validation process to complete, and then click **Create**.
- 9. Once the storage account is deployed, select **Go to resource**.
- 10. Review the **Overview** blade and the additional configurations that can be changed. These are global settings for the storage account. Notice the storage account can be used for Blob containers, File shares, Queues, and Tables.
- 11. In the **Security + networking** blade, select **Networking**. Notice **Public network access** is disabled.
 - o Select **Manage** and change the **Public network access setting to Enabled**.

ayuko01 - Microsoft Azure

Home > ayuko01_1769187659022 | Overview >

ayuko01 Storage account

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

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

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

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**

ENG US 9:06 AM 1/23/2026

Manage Azure Storage

Instructions Resources **End**

7. Review the **Encryption** tab. Notice the additional security options. Accept the defaults.

8. Select **Review + create**, wait for the validation process to complete, and then click **Create**.

9. Once the storage account is deployed, select **Go to resource**.

10. Review the **Overview** blade and the additional configurations that can be changed. These are global settings for the storage account. Notice the storage account can be used for Blob containers, File shares, Queues, and Tables.

11. In the **Security + networking** blade, select **Networking**. Notice **Public network access** is disabled.

- Select **Manage** and change the **Public network access** setting to **Enabled**.
- Change the **Public network access scope** to **Enable from selected networks**.
- In the **IPv4 Addresses** section, select **Add your client IPv4 address**.
- Save your changes.

12. In the **Data management** blade, select **Redundancy**. Notice the information about your primary and secondary data center

← Previous End →

44 Minutes Remaining

ayuko01 - Microsoft Azure

Home > ayuko01_1769187659022 | Overview > ayuko01

ayuko01 | Networking Storage account

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**

ENG US 9:09 AM 1/23/2026

Manage Azure Storage

Instructions Resources **End**

10. Review the **Overview** blade and the additional configurations that can be changed. These are global settings for the storage account. Notice the storage account can be used for Blob containers, File shares, Queues, and Tables.

11. In the **Security + networking** blade, select **Networking**. Notice **Public network access** is disabled.

- Select **Manage** and change the **Public network access** setting to **Enabled**.
- Change the **Public network access scope** to **Enable from selected networks**.
- In the **IPv4 Addresses** section, select **Add your client IPv4 address**.
- Save your changes.

12. In the **Data management** blade, select **Redundancy**. Notice the information about your primary and secondary data center locations.

13. In the **Data management** blade, select **Lifecycle management**, and then select **Add a rule**.

- Name the rule **MoveToCloud**. Notice your options for limiting the scope of the rule. Click **Next**.

← Previous End →

41 Minutes Remaining

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) *

Then

Move to cool storage

+ Add conditions

Previous Add

Manage Azure Storage

Instructions Resources

12. In the Data management blade, select Redundancy. Notice the information about your primary and secondary data center locations.

13. In the Data management blade, select Lifecycle management, and then select Add a rule.

- o Name the rule **Movetocool**. Notice your options for limiting the scope of the rule. Click Next.
- o On the Add rule page, if base blobs were last modified more than **30** days ago then **Move to cool storage**. Notice your other choices.
- o Notice you can configure other conditions. Select **Add** when you are done exploring.

Home | Lifecycle management | Add a rule ...

Add a rule

Move to cool storage

Previous End →

38 Minutes Remaining

ayuko01 | Lifecycle management

Storage account

Search + 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

Manage Azure Storage

Instructions Resources

12. In the Data management blade, select Redundancy. Notice the information about your primary and secondary data center locations.

13. In the Data management blade, select Lifecycle management, and then select Add a rule.

- o Name the rule **Movetocool**. Notice your options for limiting the scope of the rule. Click Next.
- o On the Add rule page, if base blobs were last modified more than **30** days ago then **Move to cool storage**. Notice your other choices.
- o Notice you can configure other conditions. Select **Add** when you are done exploring.

Home | Lifecycle management | Add a rule ...

Add a rule

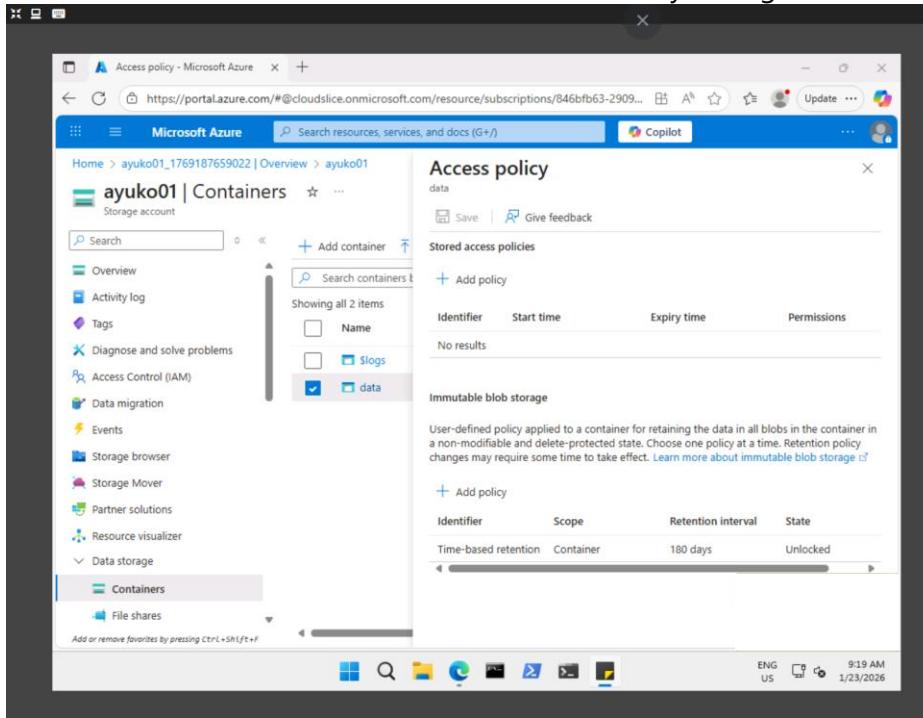
Move to cool storage

Previous End →

37 Minutes Remaining

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 menu is open, showing 'Containers' under 'Data storage'. The main area displays the 'Access policy' configuration for a container named 'ayuko01'. It shows a table for 'Stored access policies' with two items: 'Slogos' and 'data'. Below this is a section for 'Immutable blob storage' with a table showing a single policy: 'Time-based retention' with a scope of 'Container', a retention interval of '180 days', and a state of 'Unlocked'. A note states: 'User-defined policy applied to a container for retaining the data in all blobs in the container in a non-modifiable and delete-protected state. Choose one policy at a time. Retention policy changes may require some time to take effect.' A link to 'Learn more about immutable blob storage' is provided.

Manage Azure Storage

Instructions Resources

4. On your container, scroll to the ellipsis (...) on the far right, select **Access policy**.

5. In the **Immutable blob storage** area, select **Add policy**.

Setting	Value
Policy type	Time-based retention
Set retention period for	180 days

6. Select **Save**.

Manage blob uploads

1. Return to the containers page, select your **data** container and then click **Upload**.
2. On the **Upload blob** blade, expand the **Advanced** section.

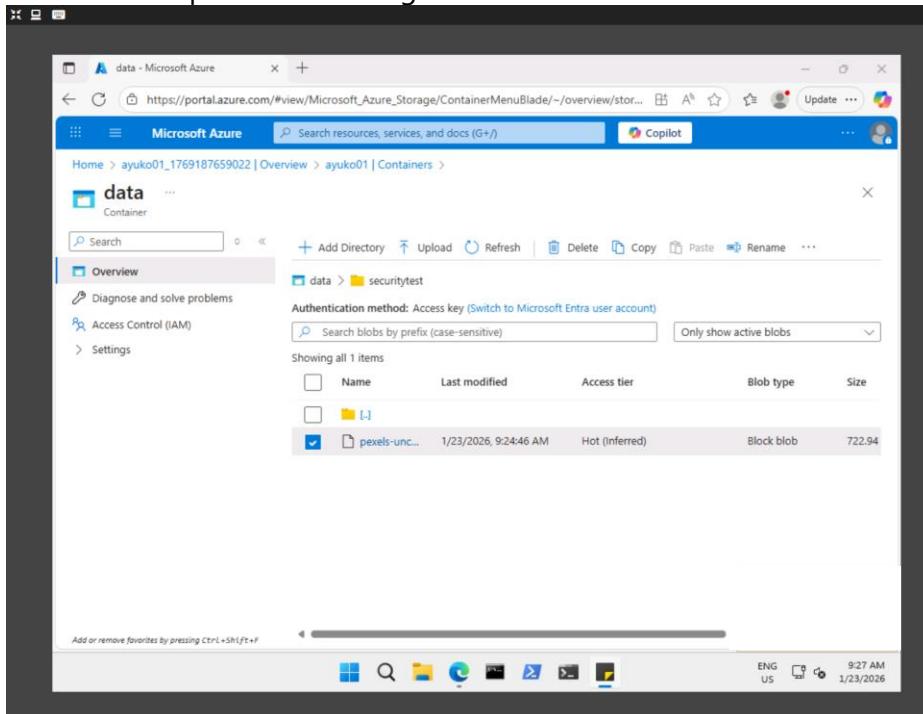
Note: Locate a file to upload. This can be any type of file, but a small file is best. A sample file can be downloaded from the AllFiles directory.

Setting	Value
Browse for file	add the file you have

← Previous End →

31 Minutes Remaining

- Blob Upload and Management



The screenshot shows the Microsoft Azure portal interface. The left navigation menu is open, showing 'Overview' under 'data' in the 'Containers' section. The main area shows a list of blobs in the 'securitytest' folder of the 'data' container. One blob, 'pixels-unc...', is selected. The 'Advanced' settings for this blob are displayed on the right, showing:

- Blob type: Block blob
- Block size: 4 MB
- Access tier: Hot (notice the other options)
- Upload to folder: securitytest
- Encryption scope: Use existing default container scope

 A note states: '3. Click **Upload**.'
 A list of steps continues:

4. Confirm you have a new folder, and your file was uploaded.
5. Select your upload file and review the ellipsis (...) options including **Download**, **Delete**, **Change tier**, and **Acquire lease**.
6. Copy the file **URL** (**Settings** → **Properties** blade) and paste into a new **InPrivate** browsing window.
7. You should be presented with an XML-formatted message stating **ResourceNotFound** or **PublicAccessNotPermitted**.

Note: This is expected, since the container you created has the public access level set to **Private** (no anonymous access).

← Previous End →

24 Minutes Remaining

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
<Code>PublicAccessNotPermitted</Code>
<Message>Public access is not permitted on this storage account. RequestId:b655dd31-a01e-008d-338e-8c5c6d000000 Time:2026-01-23T17:37:28.3609495Z</Message>
</Error>
```

Manage Azure Storage

Instructions Resources Options

Upload to folder securitytest

Encryption scope Use existing default container scope

- Click Upload.
- Confirm you have a new folder, and your file was uploaded.
- Select your upload file and review the ellipsis (...) options including Download, Delete, Change tier, and Acquire lease.
- Copy the file URL (Settings → Properties blade) and paste into a new InPrivate browsing window.
- You should be presented with an XML-formatted message stating ResourceNotFound or PublicAccessNotPermitted.

Note: This is expected, since the container you created has the public access level set to Private (no anonymous access).

Configure limited access to the blob storage

Previous End 13 Minutes Remaining

- Controlled Access to Blob Storage

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

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/pe... (redacted)

Manage Azure Storage

Instructions Resources Options

and select the ellipsis (...) to the far right, then select Generate SAS and specify the following settings (leave others with their default values):

Setting	Value
Signing key	Key 1
Permissions	Read (notice your other choices)
Start date	yesterday's date
Start time	current time
Expiry date	tomorrow's date
Expiry time	current time
Allowed IP addresses	leave blank

- Click Generate SAS token and URL.
- Copy the Blob SAS URL entry to the clipboard.
- Open another InPrivate browser window and navigate to the Blob SAS URL you copied in the previous step.

Note: You should be able to view the content of the file.

Task 3: Create and configure

Previous End 17 Minutes Remaining

A screenshot of a Windows desktop environment. On the left is a Microsoft Edge browser window displaying a vibrant bouquet of flowers (pink, yellow, blue, green) against a black background. The URL in the address bar is <https://ayuko01.blob.core.windows.net/data/securitytest/pexels-unchalee-srirugsar-14114-70330.jpg?sp...>. On the right is a "Manage Azure Storage" tool window titled "Task 3: Create and configure an Azure File storage". It contains instructions and a table for generating a SAS token.

Setting	Value
Signing key	Key 1
Permissions	Read (notice your other choices)
Start date	yesterday's date
Start time	current time
Expiry date	tomorrow's date
Expiry time	current time
Allowed IP addresses	leave blank

Instructions:

- Click Generate SAS token and URL.
- Copy the Blob SAS URL entry to the clipboard.
- Open another InPrivate browser window and navigate to the Blob SAS URL you copied in the previous step.

Note: You should be able to view the content of the file.

Task 3: Create and configure an Azure File storage

Previous End →

15 Minutes Remaining

Azure File Storage and Network Restrictions

A screenshot of the Microsoft Azure portal. On the left is a "File shares" blade for a storage account named "ayuko01_1769187659022". It shows a single file share called "share1". On the right is a "Manage Azure Storage" tool window titled "Task 3: Create and configure an Azure File storage". It shows the creation of a new file share named "share1" with the following details:

File share name	share1
Access Tier	TransactionOptimized
Protocol	SMB

Instructions:

- Click + File share and on the Basics tab give the file share a name, **share1**.
- Notice the Access tier options. Keep the default Transaction optimized.
- Move to the Backup tab and ensure Enable backup is not checked. We are disabling backup to simplify the lab configuration.
- Click Review + create, and then Create. Wait for the file share to deploy.

New file share

Validation passed

Basics Backup Review + create

Explore Storage Browser and upload a file

1. Return to your storage account and select Storage browser. The Azure Storage Browser is a portal tool that lets you quickly view all the storage services under

← Previous End →

25 Minutes Remaining

- Azure Storage Browser Usage

The screenshot shows the Azure Storage Browser interface for a storage account named 'ayuko01'. On the left, a sidebar lists various services like Data migration, Events, Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage, Security + networking, Data management, Settings, Monitoring, Monitoring (classic), Automation, and Help. The main area is titled 'Upload files' and contains a central panel with a cloud icon and the text 'Drag and drop files here or Browse for files'. Below this is a checkbox for 'Overwrite if files already exist' and a 'Upload' button. A progress bar at the bottom indicates 'OfficeIntegrator.ps1' is being uploaded at 4.85 KiB / 4.85 KiB. To the right, a sidebar titled 'Manage Azure Storage' provides instructions for using the Storage Browser, including steps for returning to the storage account, selecting file shares, and uploading files. It also includes a note about viewing file shares and managing them. At the bottom right, there are navigation buttons for 'Previous', 'End', and 'Next'.

- Network Access Restrictions for Storage Accounts

The screenshot shows the Azure portal for a deployment named 'vnet1-1769190470441'. The deployment status is 'Deployment succeeded' with a message: 'Deployment 'vnet1-1769190470441' to resource group 'az104-rg7-fod58526716' was successful.' The deployment details table shows one item: 'vnet1' of type 'Virtual network' with status 'Created'. To the right, a sidebar titled 'Manage Azure Storage' provides a numbered list of steps for setting up network access restrictions. The steps include creating a virtual network, selecting a resource group, and configuring service endpoints for Microsoft.Storage. It also covers setting up networking, managing public network access, adding existing networks, and selecting specific subnets. Navigation buttons for 'Previous', 'End', and 'Next' are at the bottom right.

vnet1 | Service endpoints

Virtual network

Search + Add Refresh

Filter service endpoints

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

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 Endpoint

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

ENG US 9:51 AM 1/23/2026

Manage Azure Storage

Instructions Resources **Virtual networks**

- In the portal, search for and select **Virtual networks**.
- Select **+ Create**. Select your resource group, and give the virtual network a name, **vnet1**.
- Take the defaults for other parameters, select **Review + create**, and then **Create**.
- Wait for the virtual network to deploy, and then select **Go to resource**.
- In the **Settings** section, select the **Service endpoints** blade.
 - Select **Add**.
 - In the **Service** drop-down select **Microsoft.Storage**.
 - In the **Subnets** drop-down check the **Default** subnet.
 - Click **Add** to save your changes.
- Return to your storage account.
- In the **Security + networking** blade, select **Networking**.
- Under **Public network access** select **Manage**.
- Select **Add a virtual network** and then **Add existing network**.
- Select **vnet1** and **default** subnet, select **Add**.

Previous End → 14 Minutes Remaining

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](#)

Save Cancel

ENG US 9:54 AM 1/23/2026

Manage Azure Storage

Instructions Resources **Networking**

- Under **Public network access** select **Manage**.
- Select **Add a virtual network** and then **Add existing network**.
- Select **vnet1** and **default** subnet, select **Add**.
- In the **IPv4 Addresses** section, Delete your machine IP address. Allowed traffic should only come from the virtual network.
- Be sure to **Save** your changes.

Note: The storage account should now only be accessed from the virtual network you just created.

- Select the **Storage browser** and **Refresh** the page. Navigate to your file share or blob content.

Note: You should receive a message *not authorized to perform this operation*. You are not connecting from the virtual network. It may take a couple of minutes for this to take effect. You may still be able to view the file share, but not the files or blobs in it.

Previous End → 11 Minutes Remaining

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is open, showing the 'Networking' section under 'Security + networking'. The main content area displays the 'ayuko01 | Networking' page for a Storage account. It includes sections for 'Public network access' (Enabled from selected networks), 'Network security perimeter' (No network security perimeter has been associated), and 'Resource settings: Virtual networks, IP addresses, and exceptions' (Access rules: None, Virtual networks: 1, IPv4 addresses: None, Exceptions: 1). A note at the bottom states: 'This request is not authorized to perform this operation.'

Manage Azure Storage

Instructions Resources

11. In the **IPv4 Addresses** section, **Delete** your machine IP address. Allowed traffic should only come from the virtual network.

12. Be sure to **Save** your changes.

Note: The storage account should now only be accessed from the virtual network you just created.

13. Select the **Storage browser** and **Refresh** the page. Navigate to your file share or blob content.

Note: You should receive a message *not authorized to perform this operation*. You are not connecting from the virtual network. It may take a couple of minutes for this to take effect. You may still be able to view the file share, but not the files or blobs in the storage account.

This request is not authorized to perform this operation.

Summary

Session ID: 43104642ff0064bea4913675eb84ebcb...	Resource ID: /subscriptions/846fbfb63-2909-4efc-8bd...
Extension: Microsoft_Azure_Storage	Content: Fileblade
Error code: 403	Storage Request ID: 56759ba4ef1a-0045-4f9f-57bc0d800000

Previous End 25 Minutes Remaining

The screenshot shows the Microsoft Azure portal interface. The navigation menu is open, showing the 'Storage browser' section under 'Data storage'. The main content area displays the 'ayuko01 | Storage browser' page for a Storage account. It includes sections for 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage browser' (selected), 'Storage Mover', 'Partner solutions', 'Resource visualizer', and 'Data storage'. A note at the top states: 'Help me save costs by tiering unused blobs.' Below it, a cloud icon indicates: 'This request is not authorized to perform this operation.' The summary table shows details about the failed request.

Manage Azure Storage

Instructions Resources

13. Select the **Storage browser** and **Refresh** the page. Navigate to your file share or blob content.

Note: You should receive a message *not authorized to perform this operation*. You are not connecting from the virtual network. It may take a couple of minutes for this to take effect. You may still be able to view the file share, but not the files or blobs in the storage account.

This request is not authorized to perform this operation.

Summary

Session ID: 43104642ff0064bea4913675eb84ebcb...	Resource ID: /subscriptions/846fbfb63-2909-4efc-8bd...
Extension: Microsoft_Azure_Storage	Content: Fileblade
Error code: 403	Storage Request ID: 56759ba4ef1a-0045-4f9f-57bc0d800000

Details

- This request is not authorized to perform this operation. RequestId:56759ba4ef1a-0045-4f9f-57bc0d800000 Date:2024-02-20T07:57:00Z CorrelationId:730025-5e20-433a-9700-259810000000
- The request failed because: You are not connecting from the virtual network. This may be blocking access to storage services. Try adding your client IP address (168.243.203.346) to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. Learn more

Cleanup your resources

Previous End 22 Minutes Remaining