

# 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.

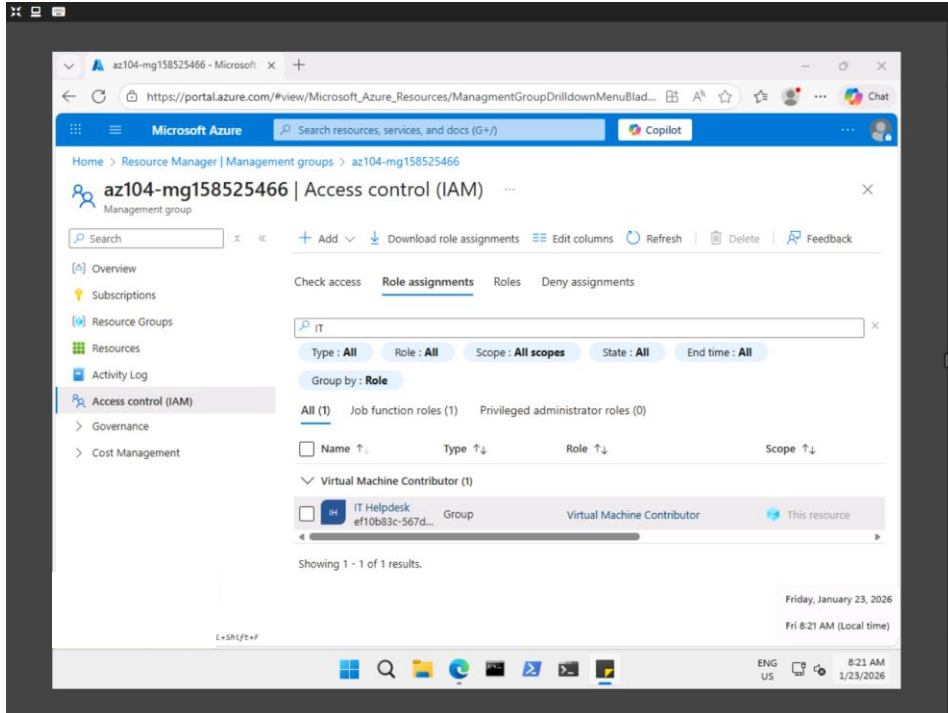
### Management Groups and Subscription Structure

The screenshot displays the Azure Portal interface. The main pane shows the 'Management groups' blade under 'Resource Manager'. It lists three management groups: 'Tenant Root Group', 'az104-mg158525466', and 'LOD'. The 'az104-mg158525466' group is selected, showing its details. The sidebar on the right contains instructions for creating and managing management groups, including a table for settings and a note about the root management group.

Setting	Value
Management group ID	az104-mg158525466 (must be unique in the directory)
Management group display name	az104-mg158525466

**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



Manage Subscriptions and RBAC

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 This has been replaced by the **Azure Resource Manager** deployment model.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.

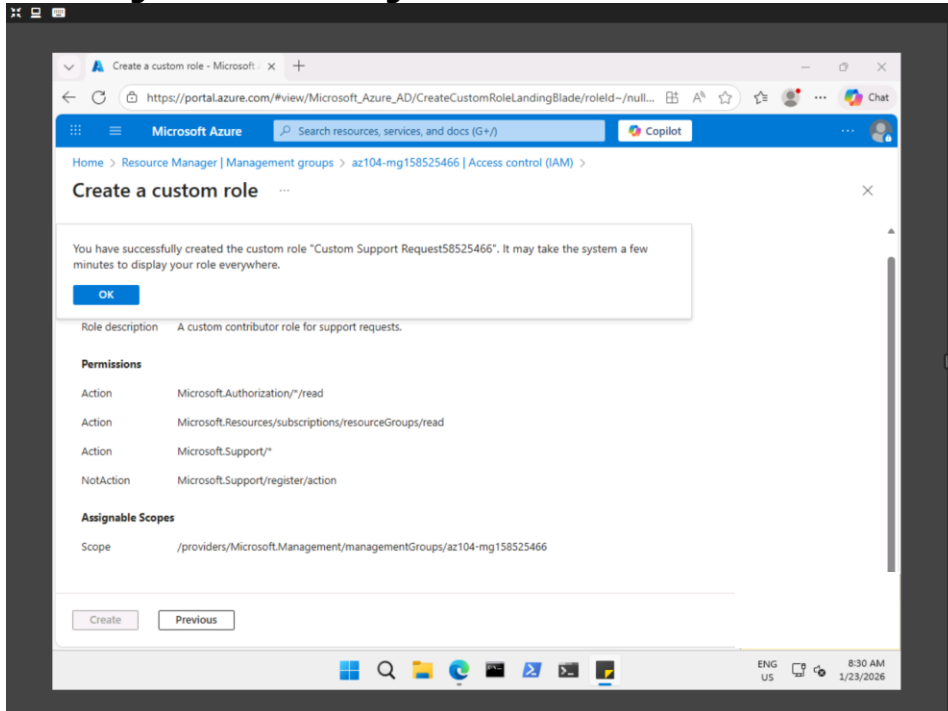
**Note:** As a best practice always assign roles to groups not individuals.

**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.

Previous End

41 Minutes Remaining

## Role Assignment Monitoring



Manage Subscriptions and RBAC

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**

Previous End

32 Minutes Remaining



ayuko01 - Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > ayuko01\_1769187659022 | Overview >

ayuko01

Storage account

Search

PropertiesMonitoringCapabilities (7)Recommendations (0)TutorialsTools + 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

Manage Azure Storage

InstructionsResources

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

PreviousEnd

44 Minutes Remaining

ayuko01 - Microsoft Azure

Search resources, services, and docs (G+J)

Copilot

Home > ayuko01\_1769187659022 | Overview > ayuko01

ayuko01 | Networking

Storage account

Search

Public accessPrivate endpointsNetwork routingCustom 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

Manage Azure Storage

InstructionsResources

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.

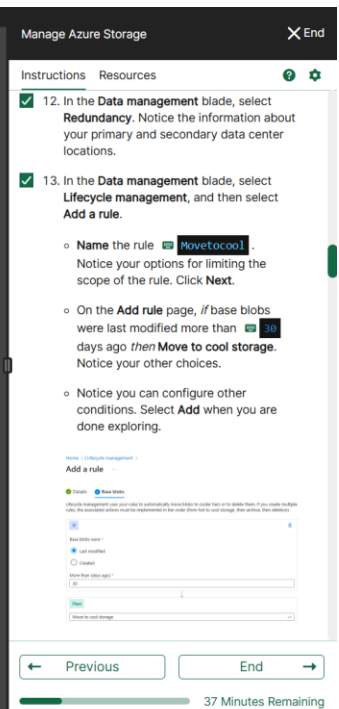
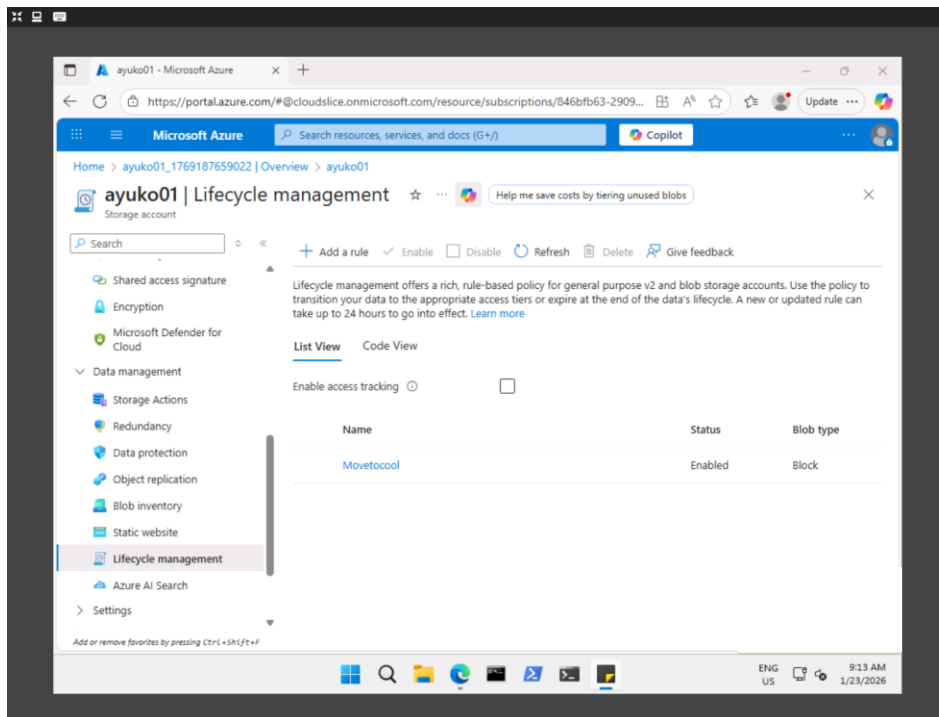
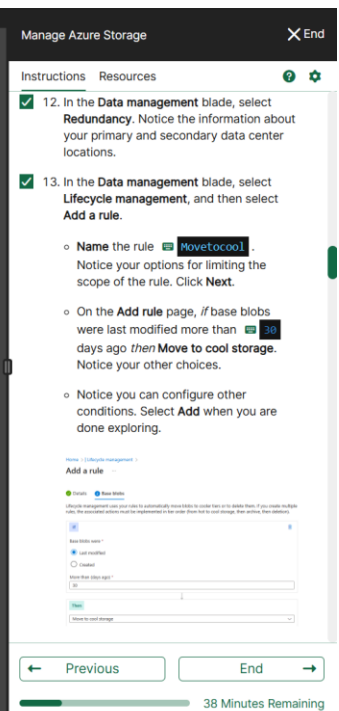
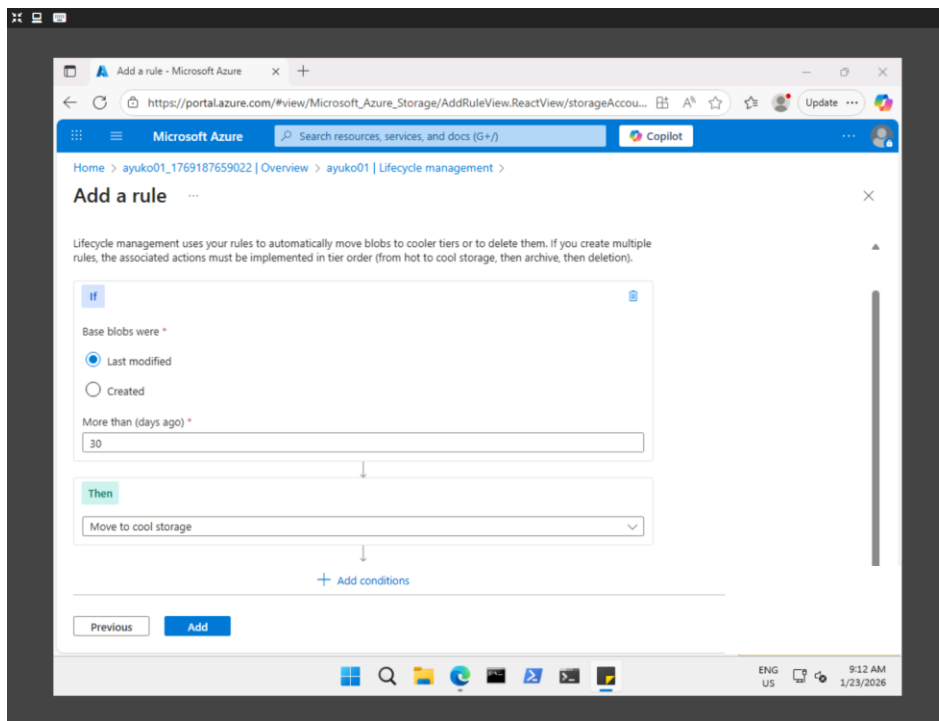
12. In the **Data management** blade, select **Redundancy**. Notice the information about your primary and secondary data center locations.

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

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

PreviousEnd

41 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 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 shows a table with columns: Identifier, Start time, Expiry time, and Permissions. 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'.

On the right, the 'Manage Azure Storage' sidebar is open, showing instructions for configuring the policy. The instructions include:

- 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**.

The sidebar also shows a table with columns: Setting, Value. The table contains one entry: 'Policy type' with a value of 'Time-based retention'. Below this, the 'Set retention period for' is set to '180 days'.

At the bottom of the sidebar, there is a 'Manage blob uploads' section with instructions:

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

A note is provided: '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.'

The sidebar also shows a table with columns: Setting, Value. The table contains one entry: 'Browse for file' with a value of 'add the file you have selected to upload'.

At the bottom of the sidebar, there are buttons for 'Previous' and 'End', and a progress bar indicating '31 Minutes Remaining'.

### - Blob Upload and Management

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 'data' container overview. The 'Overview' section shows a table with columns: Name, Last modified, Access tier, Blob type, and Size. The table contains one entry: 'pexels-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'.

On the right, the 'Manage Azure Storage' sidebar is open, showing instructions for uploading and managing blobs. The instructions include:

- 3. Click **Upload**.
- 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**.

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

The sidebar also shows a table with columns: Setting, Value. The table contains one entry: 'Blob type' with a value of 'Block blob'. Below this, the 'Block size' is set to '4 MIB', the 'Access tier' is set to 'Hot (notice the other options)', the 'Upload to folder' is set to 'securitytest', and the 'Encryption scope' is set to 'Use existing default container scope'.

At the bottom of the sidebar, there are buttons for 'Previous' and 'End', and a progress bar indicating '24 Minutes Remaining'.

ayuko01.blob.core.windows.net/

https://ayuko01.blob.core.windows.net/data/securitytest/pexels-unchalee-srugsar-14114-70330.jpg

InPrivate

Update

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

Upload to folder securitytest

Encryption scope Use existing default container scope

3. Click Upload.

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).

Configure limited access to the blob storage

Previous End

13 Minutes Remaining

- Controlled Access to Blob Storage

Generate SAS - Microsoft Azure

https://portal.azure.com/#view/Microsoft\_Azure\_Storage/ContainerMenuBlade/~/overview/stor...

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > ayuko01\_1769187659022 | Overview > ayuko01 | Contain...

data

Container

Search

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

data > securitytest

Authentication method:

Search blobs by pr

Sorting all 1 items

ified

Acces

6, 9:24:46 AM Hot

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

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

Blob SAS token

sp=r&st=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-srugsar-...

Manage Azure Storage

Instructions Resources

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

2. Click Generate SAS token and URL.

3. Copy the Blob SAS URL entry to the clipboard.

4. 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

pxels-unchalee-sirugsar-14114

https://ayuko01.blob.core.windows.net/data/securitytest/pxels-unchalee-sirugsar-14114-70330.jpg?sp... InPrivate Update



ENG US 9:36 AM 1/23/2026

Manage Azure Storage

Instructions Resources

and select the endpoint (URL) to the left, 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

☒

2. Click **Generate SAS token and URL**.

☒

3. Copy the **Blob SAS URL** entry to the clipboard.

☒

4. 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

share1 - Microsoft Azure

https://portal.azure.com/#view/Microsoft\_Azure\_FileStorage/FileShareMenuBlade/~/\_overview/id... Update

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > ayuko01\_1769187659022 | Overview > ayuko01 | File shares > New file share >

share1

SMB File share

Search

Connect Upload Refresh Add directory Delete share Change tier

Overview

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Enable Backup for file share "share1" to protect your data. [Learn more](#)

Essentials

JSON View

Storage account

ayuko01

Resource group (move)

az104-r97-1od58526716

Location

East US

Primary/Secondary location

Primary: East US, Secondary: West US

Subscription (move)

AZ-104T00A\_CSR\_3

Subscription ID

846bf63-2909-4efc-8bd7-d0d2d465a22a

Share URL

https://ayuko01.file.core.windows.net/share1

Redundancy

Geo-redundant storage (GRS)

Configuration modified

1/23/2026, 9:40:12 AM

Properties

Capabilities (2)

Tutorials

Manage Azure Storage

Instructions Resources

☒

2. Click **File share** and on the **Basics** tab give the file share a name, **share1**.

☒

3. Notice the **Access tier** options. Keep the default **Transaction optimized**.

☒

4. Move to the **Backup** tab and ensure **Enable backup** is not checked. We are disabling backup to simplify the lab configuration.

☒

5. Click **Review + create**, and then **Create**. Wait for the file share to deploy.

Home > az104demo123897 | File shares >

New file share

Validation passed

Basics Backup Review + create

Basics

File share name

share1

Access Tier

TransactionOptimized

Protocol

SMB

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

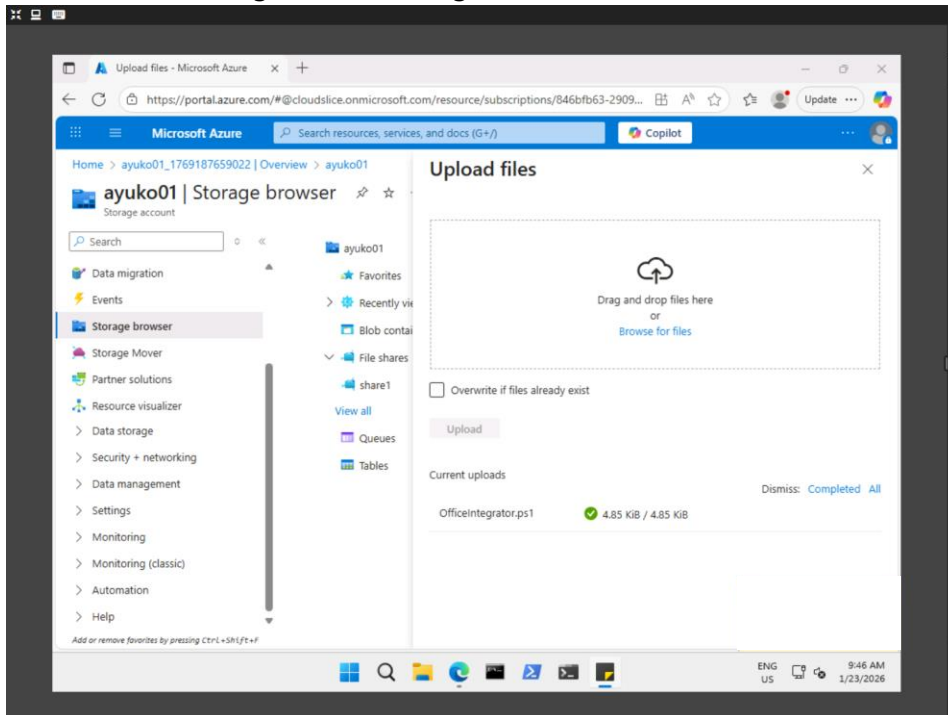
Previous

End

25 Minutes Remaining



## - Azure Storage Browser Usage



The screenshot shows the Azure Storage Browser interface. The main area displays an 'Upload files' dialog with a large dashed box for dragging and dropping files. Below this, there's a section for 'Current uploads' showing a file named 'Officeintegrator.ps1' with a size of 4.85 KiB. The left sidebar contains a search bar and a list of storage services including Data migration, Events, Storage browser (selected), Storage Mover, Partner solutions, Resource visualizer, Data storage, Security + networking, Data management, Settings, Monitoring, Monitoring (classic), Automation, and Help. The right sidebar shows the 'Manage Azure Storage' pane with instructions for exploring the Storage Browser and uploading a file.

**Instructions**

- 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 your account.
- 2. Select **File shares** and verify your **share1** directory is present.
- 3. Select your **share1** directory and notice you can **+ Add directory**. This lets you create a folder structure.
- 4. Select **Upload**. Browse to a file of your choice, and then click **Upload**.

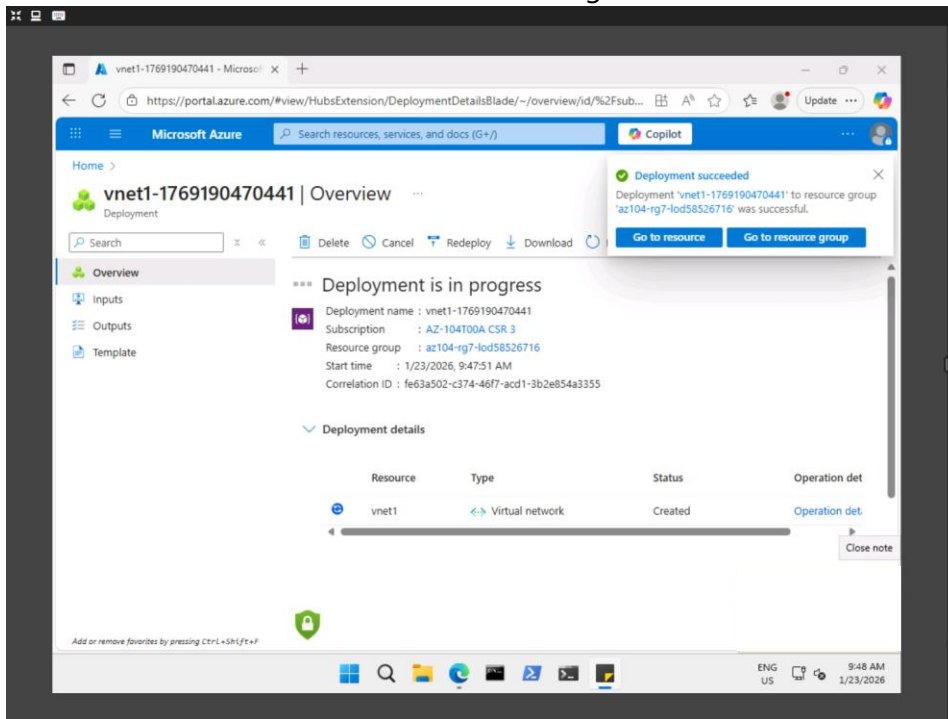
**Note:** You can view file shares and manage those shares in the Storage Browser. There are currently no restrictions.

**Restrict network access to the storage account**

Previous End

20 Minutes Remaining

## - Network Access Restrictions for Storage Accounts



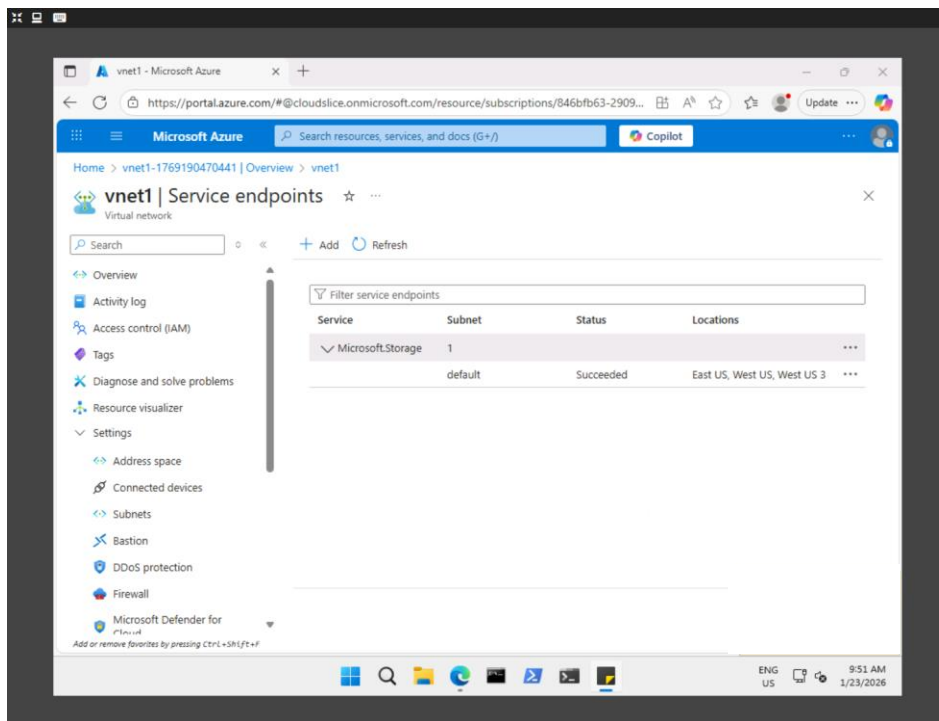
The screenshot shows the Azure portal interface. The main area displays the 'vnet1-1769190470441 | Overview' page. A deployment status message indicates 'Deployment succeeded' for the resource group 'az104-rg7-lod58526716'. The deployment details table shows the resource 'vnet1' of type 'Virtual network' with a status of 'Created'. The right sidebar shows the 'Manage Azure Storage' pane with instructions for network access restrictions.

**Instructions**

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

Previous End

18 Minutes Remaining



Manage Azure Storage

End

Instructions

Resources

1. In the portal, search for and select **virtual networks**.

2. Select **Create**. Select your resource group, and give the virtual network a name, **vnet1**.

3. Take the defaults for other parameters, select **Review + create**, and then **Create**.

4. Wait for the virtual network to deploy, and then select **Go to resource**.

5. 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.

6. Return to your storage account.

7. In the **Security + networking** blade, select **Networking**.

8. Under **Public network access** select **Manage**.

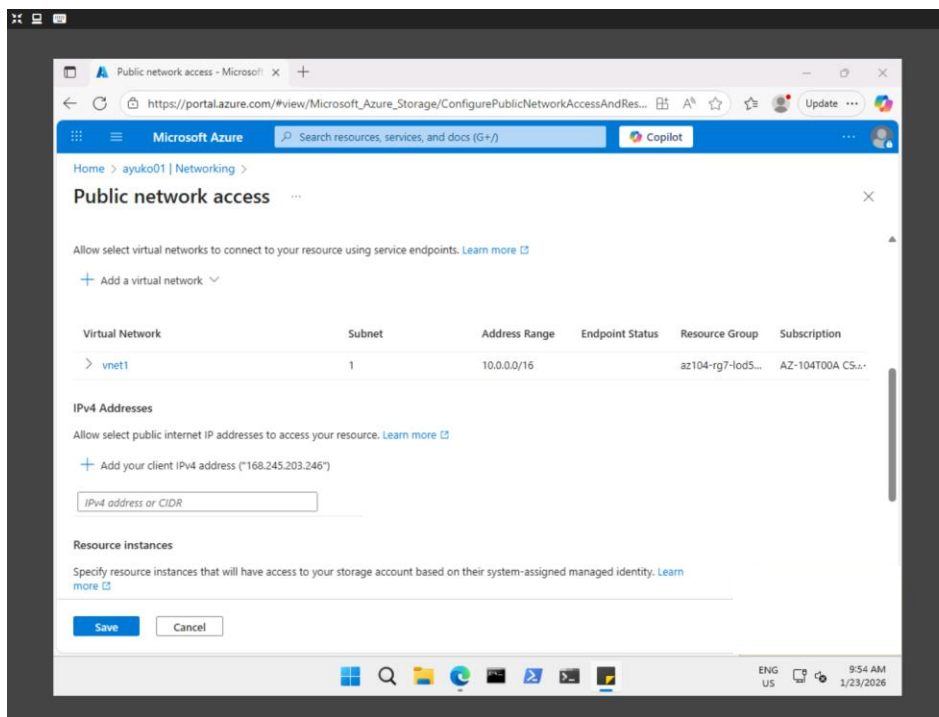
9. Select **Add a virtual network** and then **Add existing network**.

10. Select **vnet1** and **default** subnet, select

Previous

End

14 Minutes Remaining



Manage Azure Storage

End

Instructions

Resources

Networking:

8. Under **Public network access** select **Manage**.

9. Select **Add a virtual network** and then **Add existing network**.

10. Select **vnet1** and **default** subnet, select **Add**.

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

Previous

End

11 Minutes Remaining

