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.

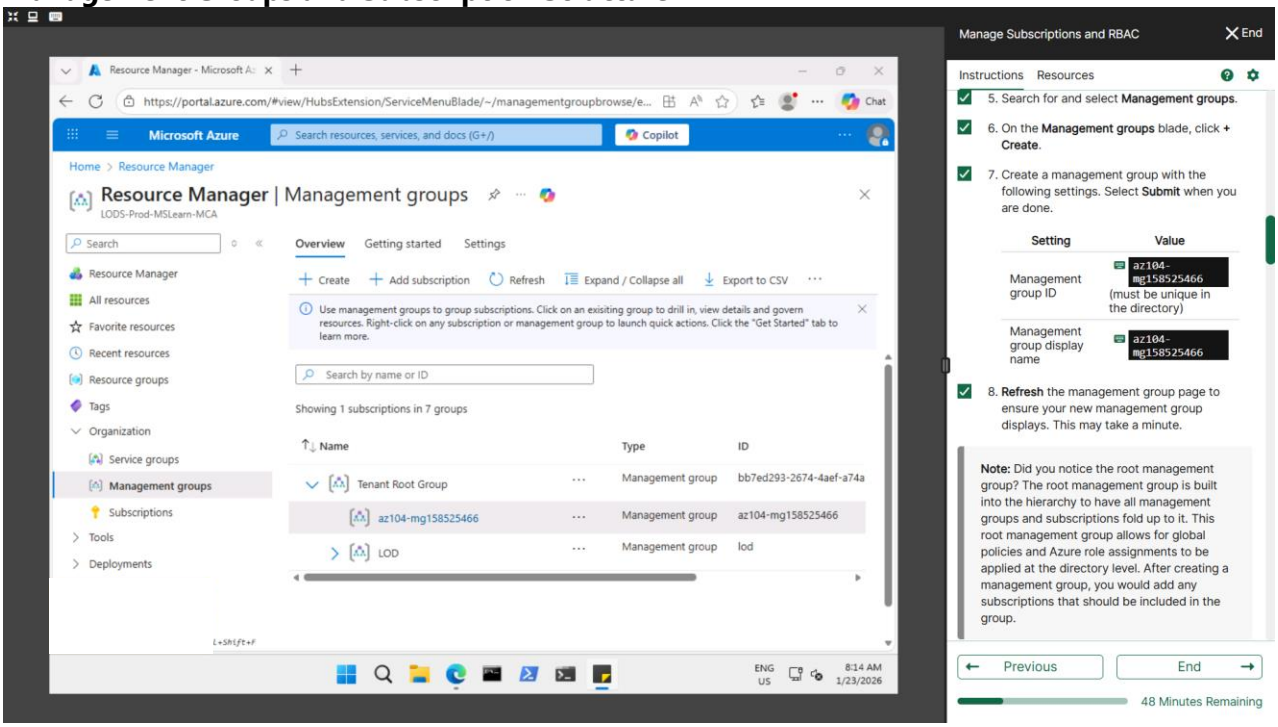
- Implemented governance, access control, and secure storage best practices

---

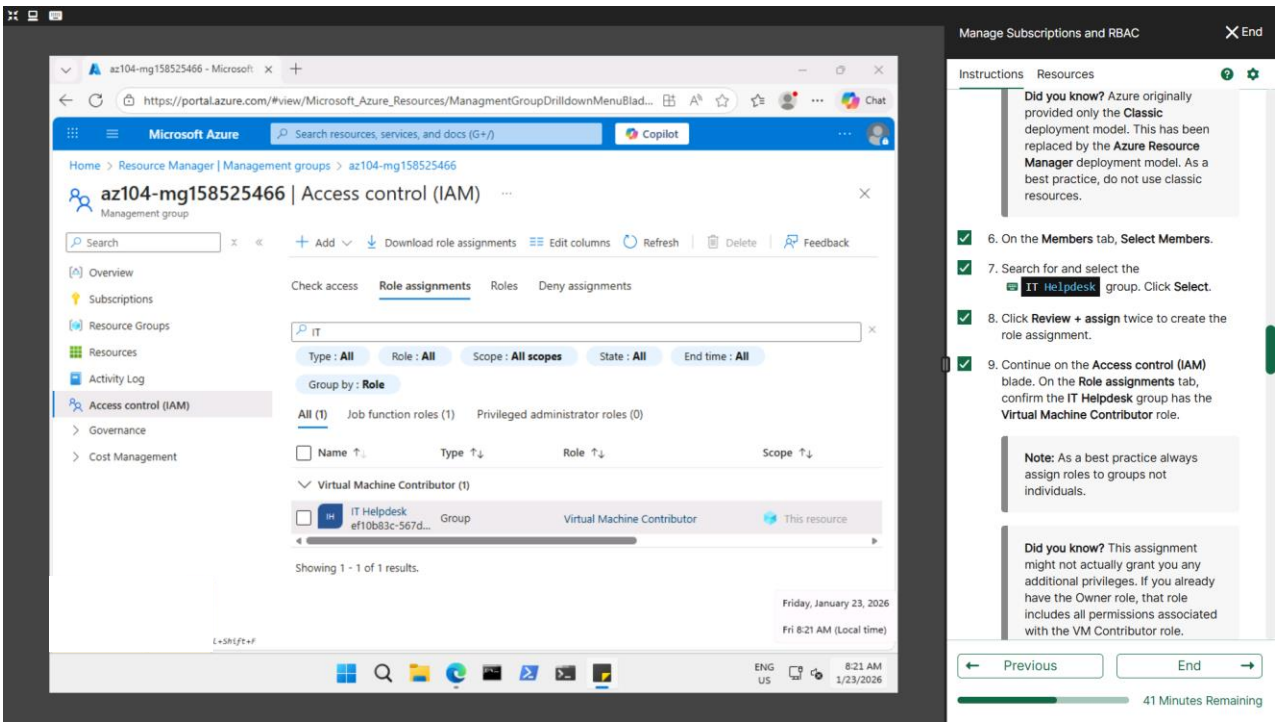
Subscription Governance and Role-Based Access Control (RBAC)

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.

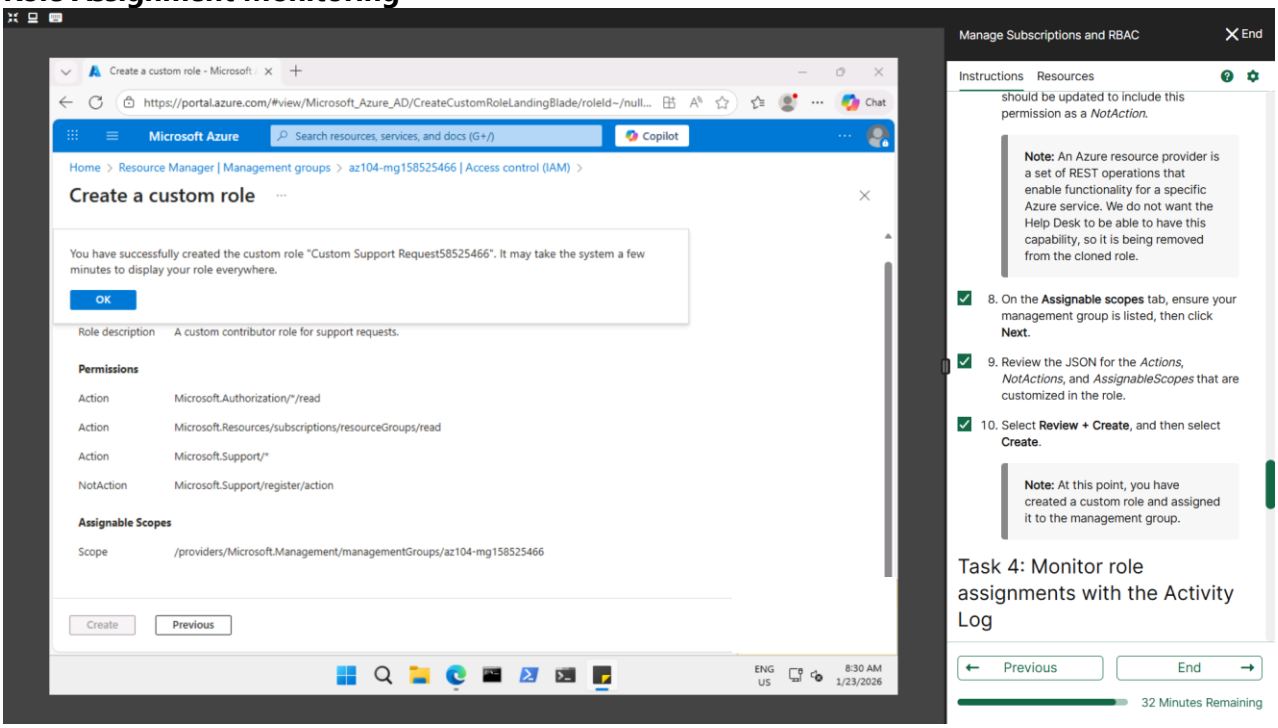
Management Groups and Subscription Structure

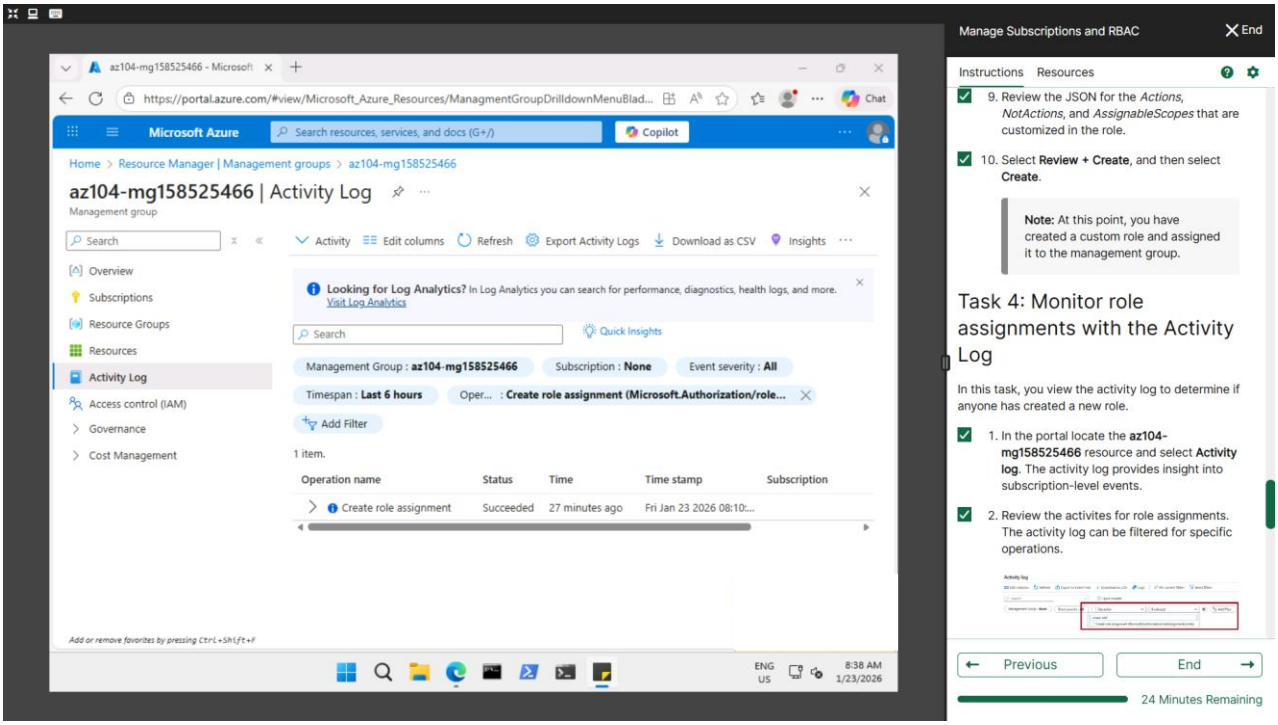


Built-in and Custom RBAC Roles



Role Assignment Monitoring

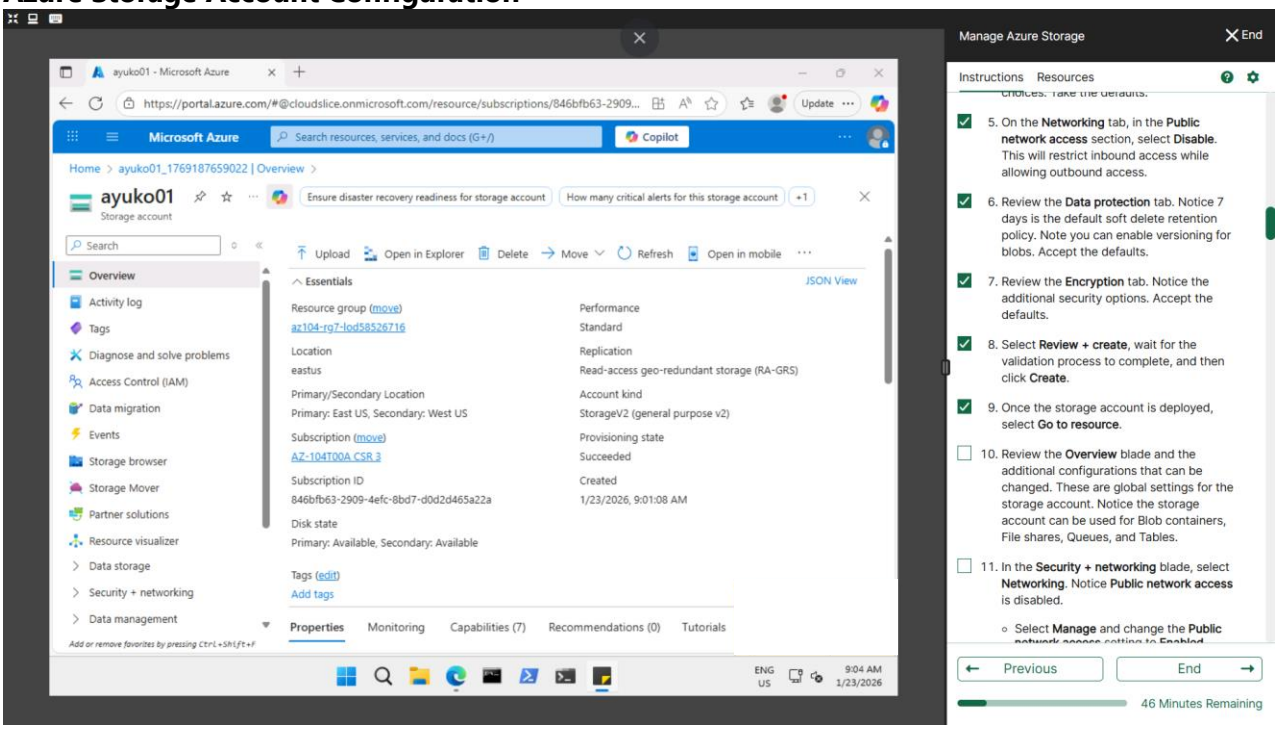


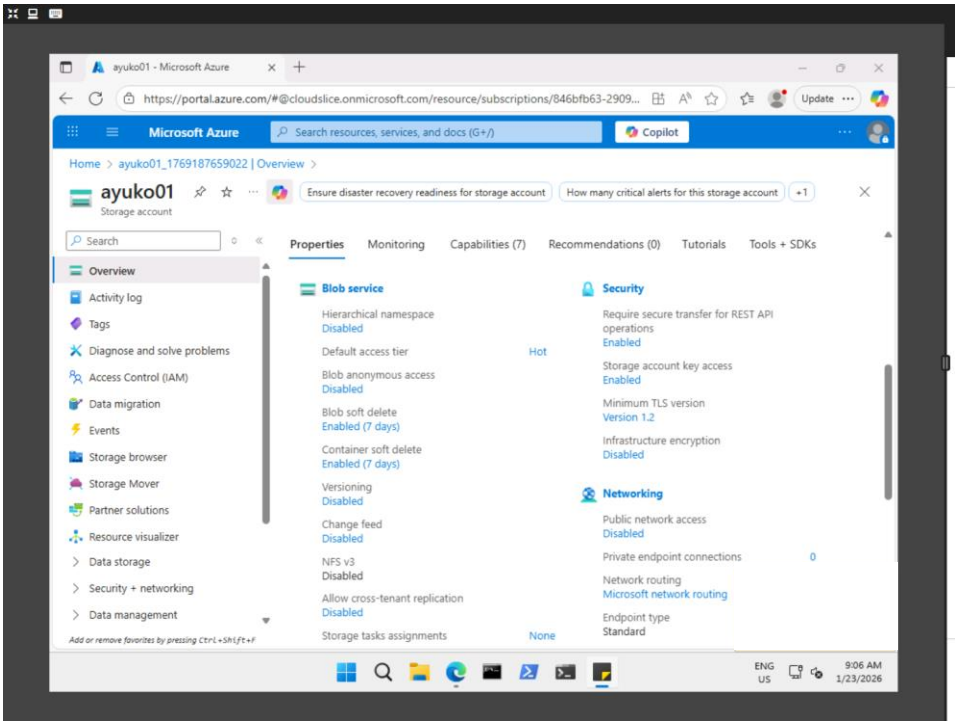


Secure Azure Storage Configuration

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





Manage Azure Storage

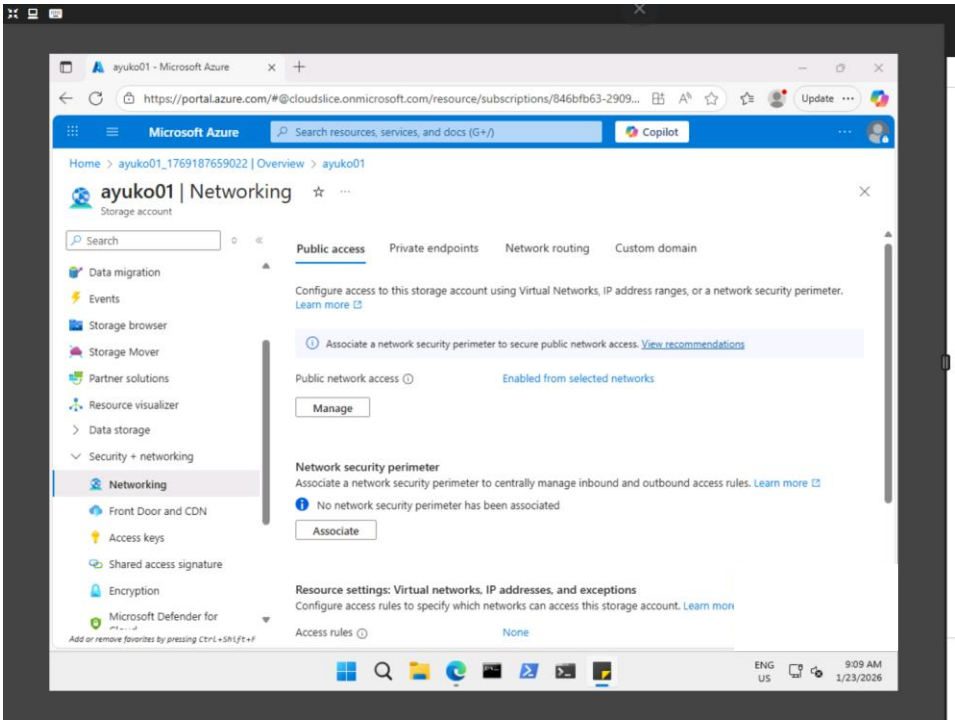
End

Instructions Resources

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



Manage Azure Storage

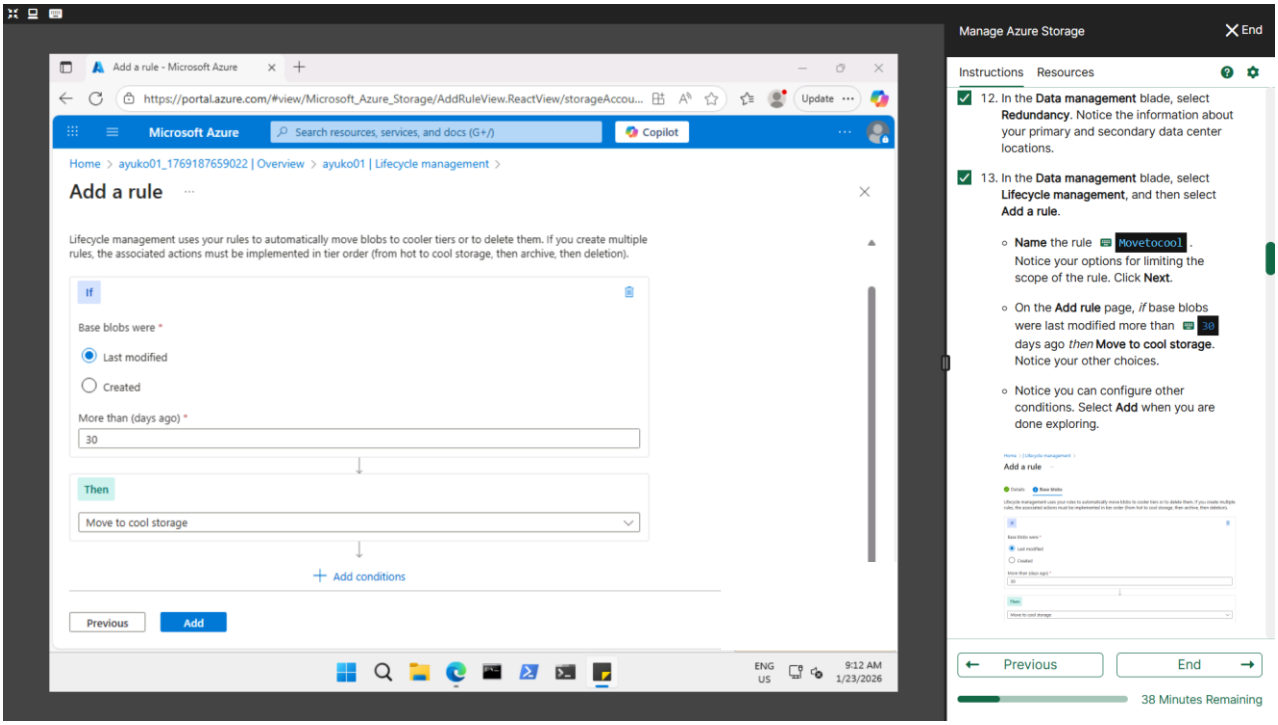
End

Instructions Resources

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 `Movetocool`. Notice your options for limiting the scope of the rule. Click **Next**.

Previous End

41 Minutes Remaining



Manage Azure Storage

End

Instructions Resources

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

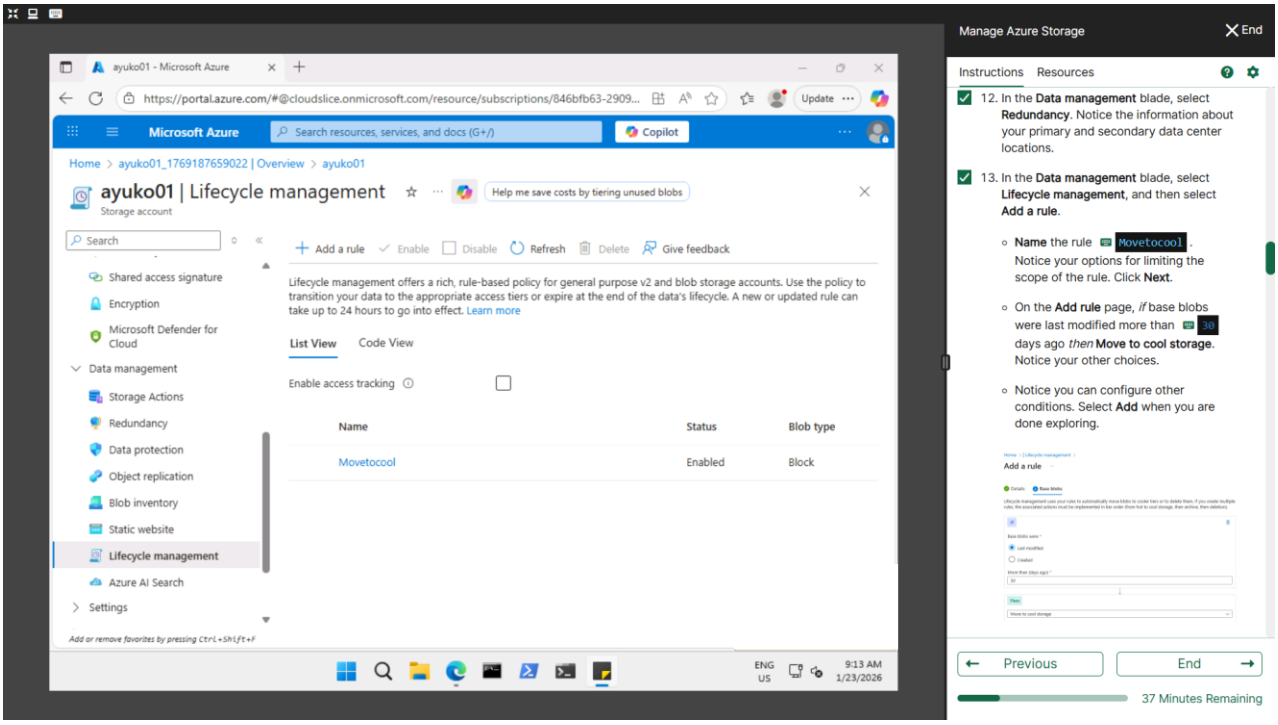
13. In the **Data management** blade, select **Lifecycle management**, and then select **Add a rule**.

    - **Name** the rule `Movetocool`. Notice your options for limiting the scope of the rule. Click **Next**.
    - 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.
    - Notice you can configure other conditions. Select **Add** when you are done exploring.

Previous

End

38 Minutes Remaining



Manage Azure Storage

End

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**.

    - **Name** the rule `Movetocool`. Notice your options for limiting the scope of the rule. Click **Next**.
    - 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.
    - Notice you can configure other conditions. Select **Add** when you are done exploring.

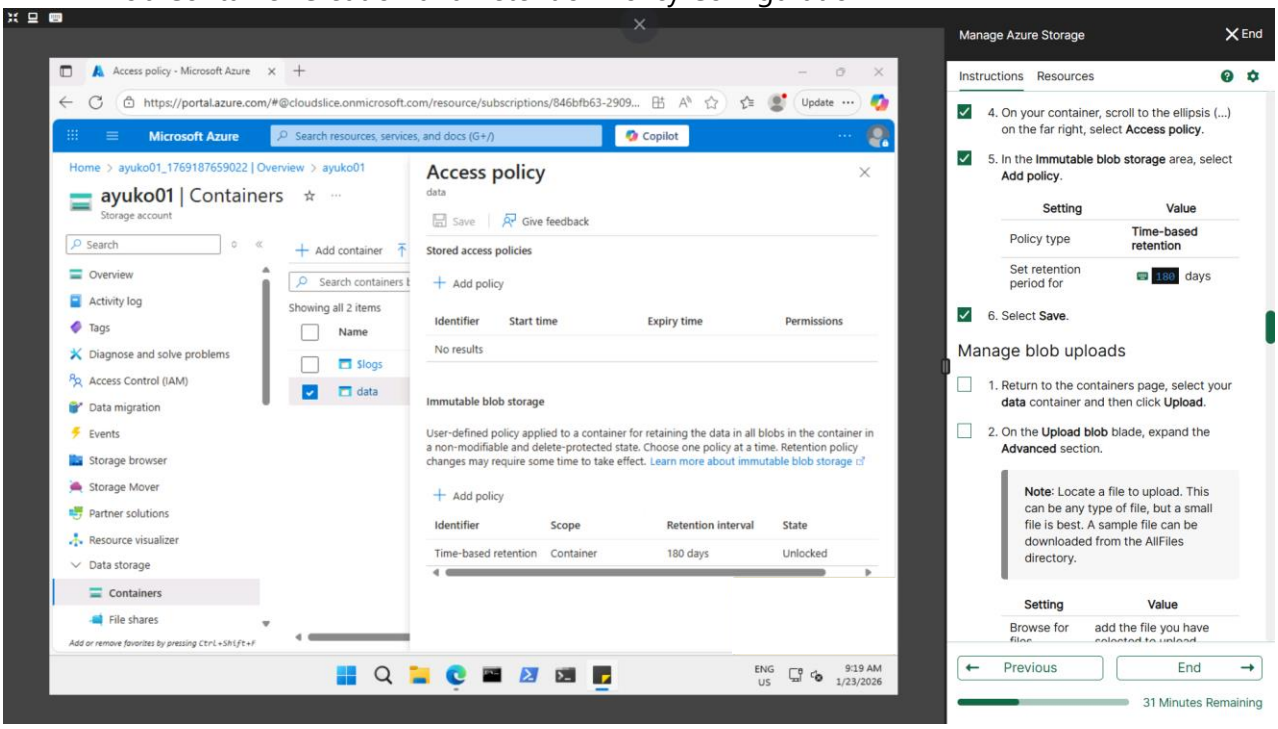
Previous

End

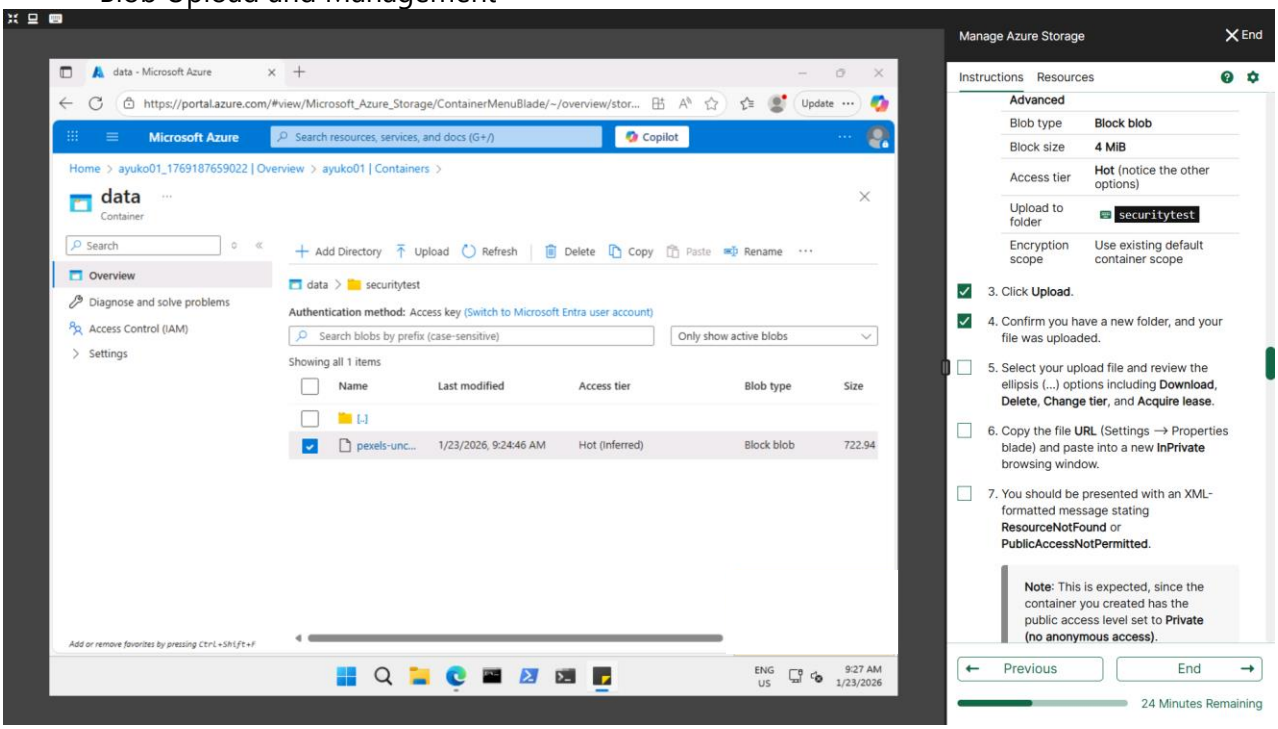
37 Minutes Remaining

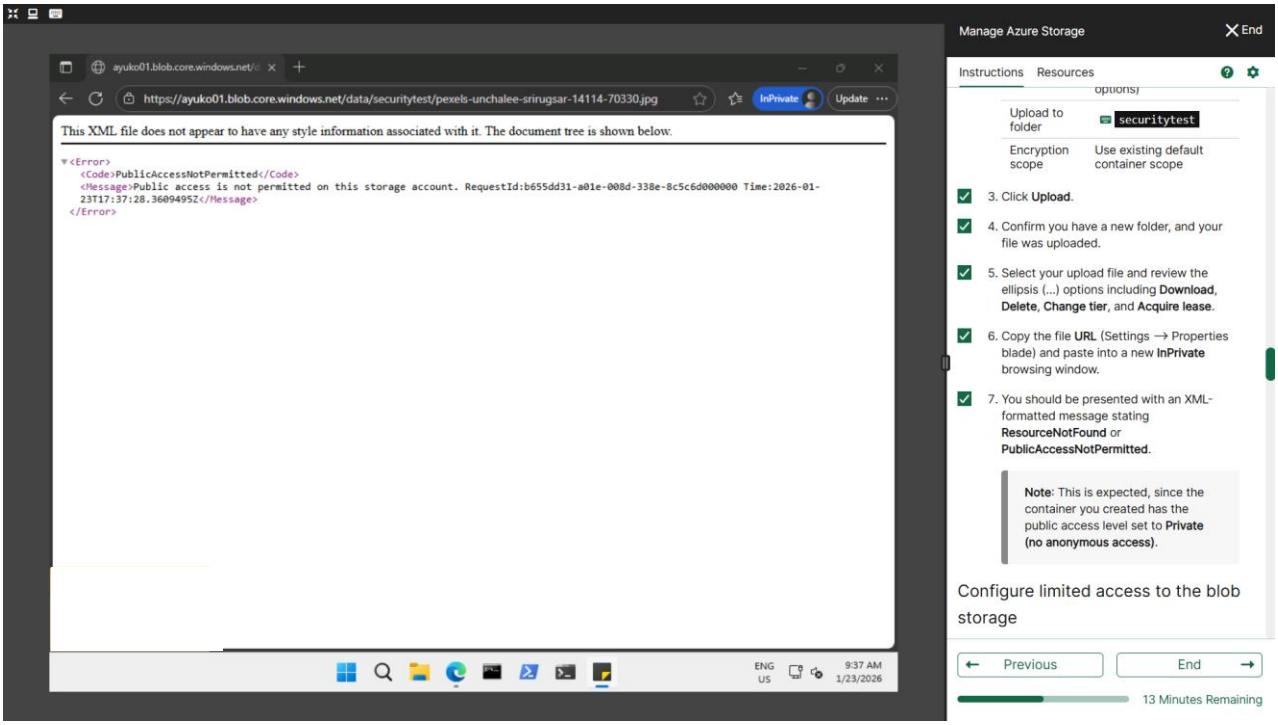
Secure Blob Storage and Retention Policies

- Blob Container Creation and Retention Policy Configuration

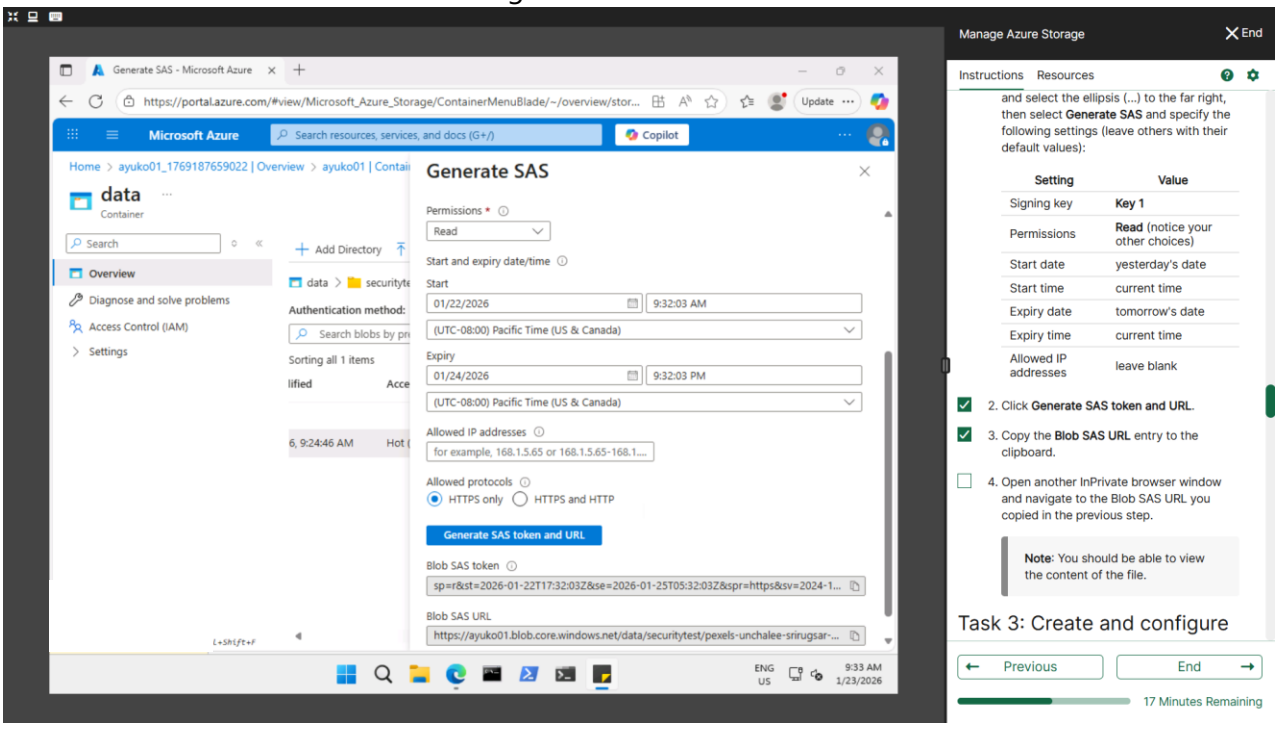


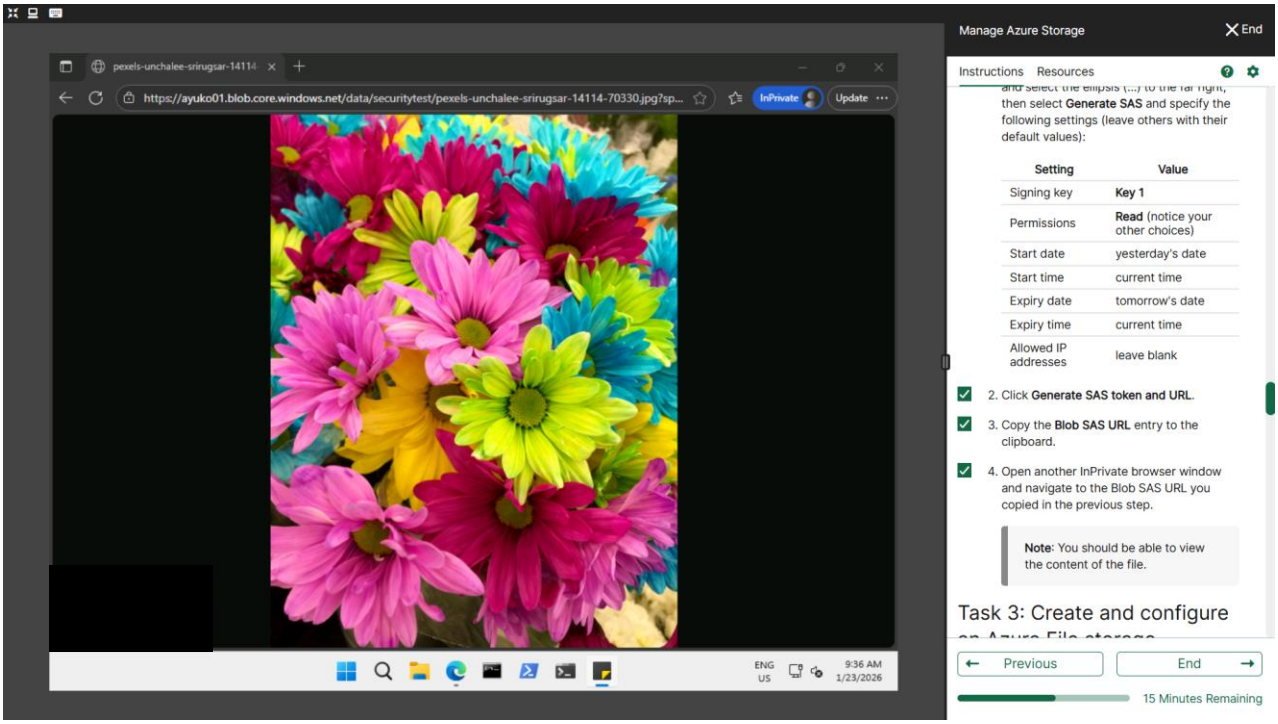
- Blob Upload and Management



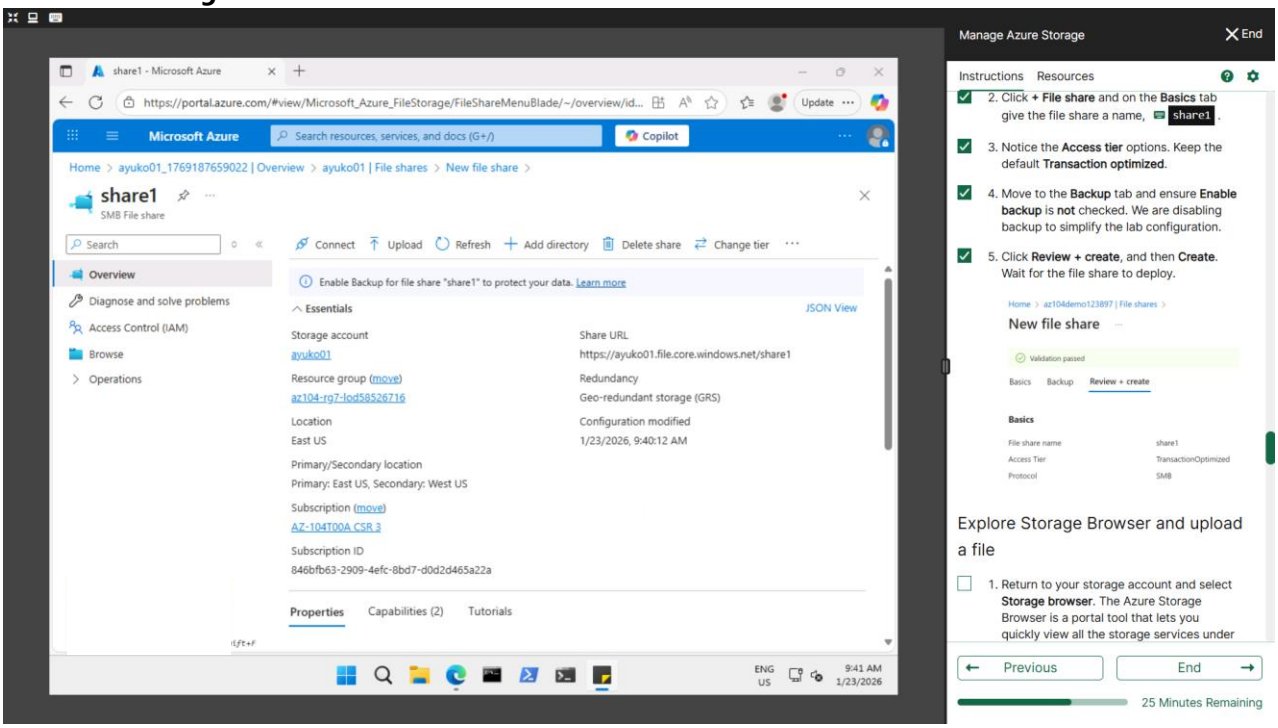


- Controlled Access to Blob Storage

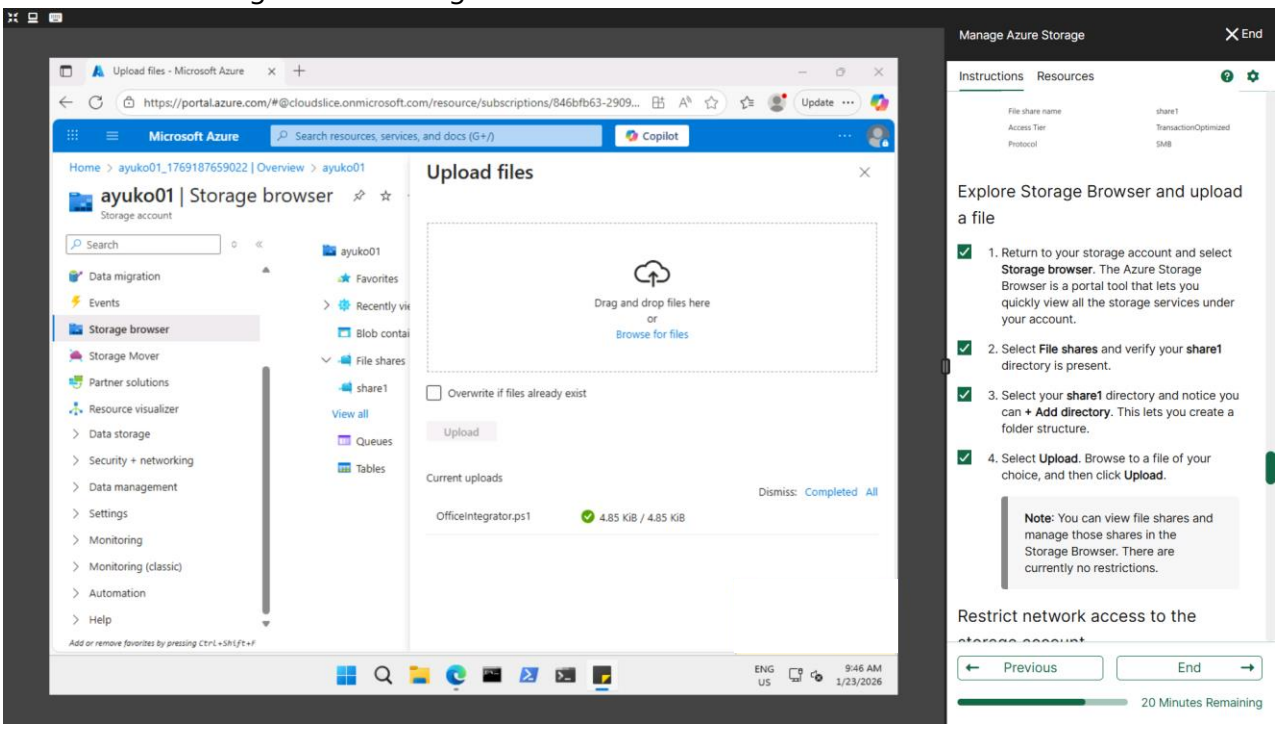




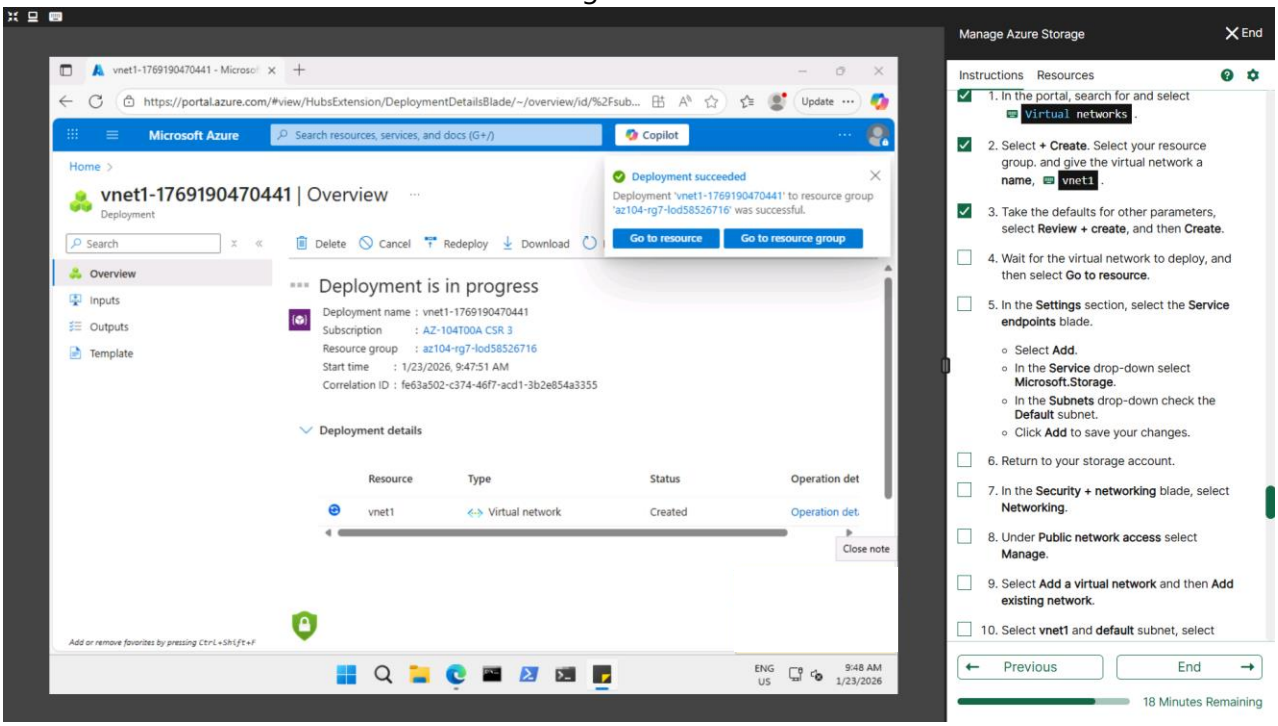
Azure File Storage and Network Restrictions

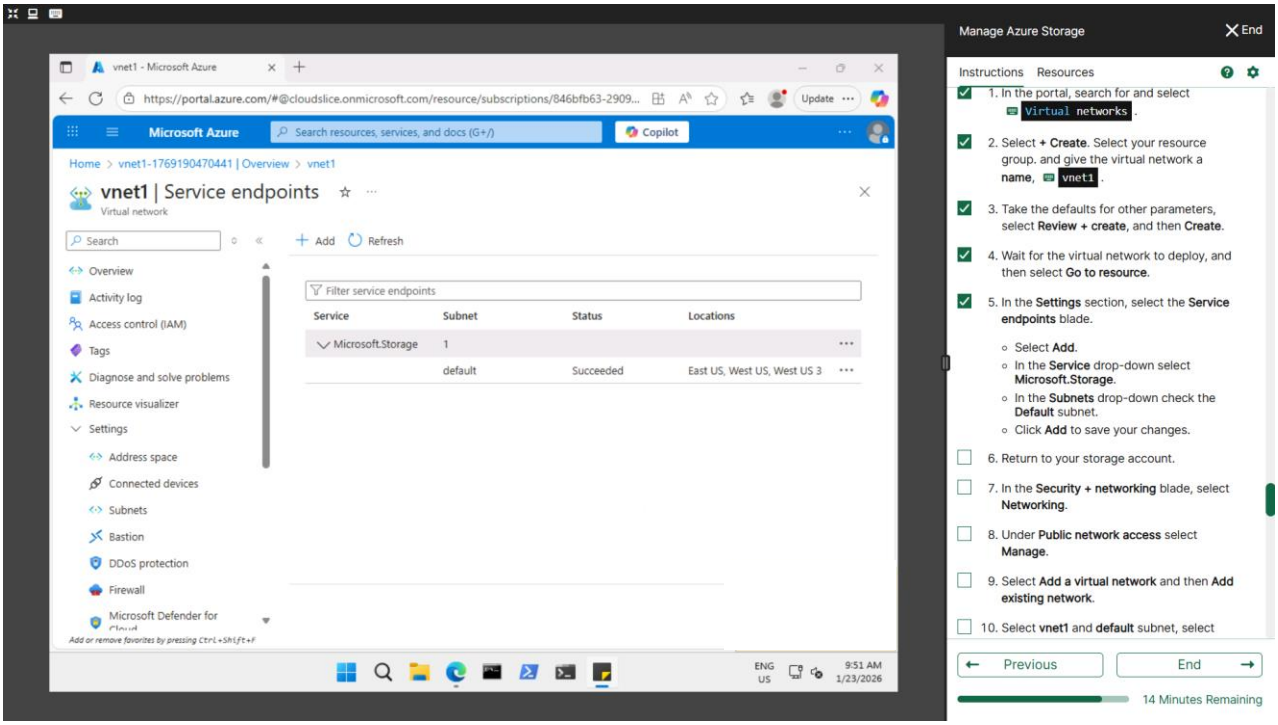


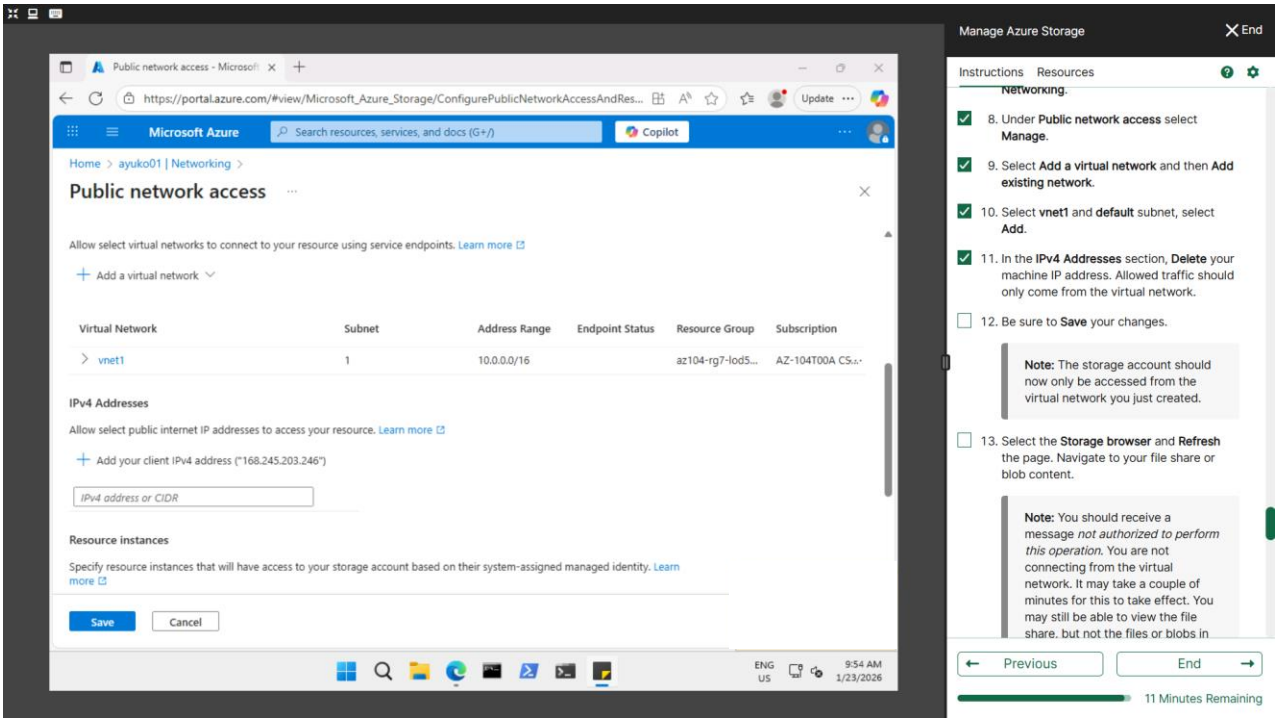
- Azure Storage Browser Usage

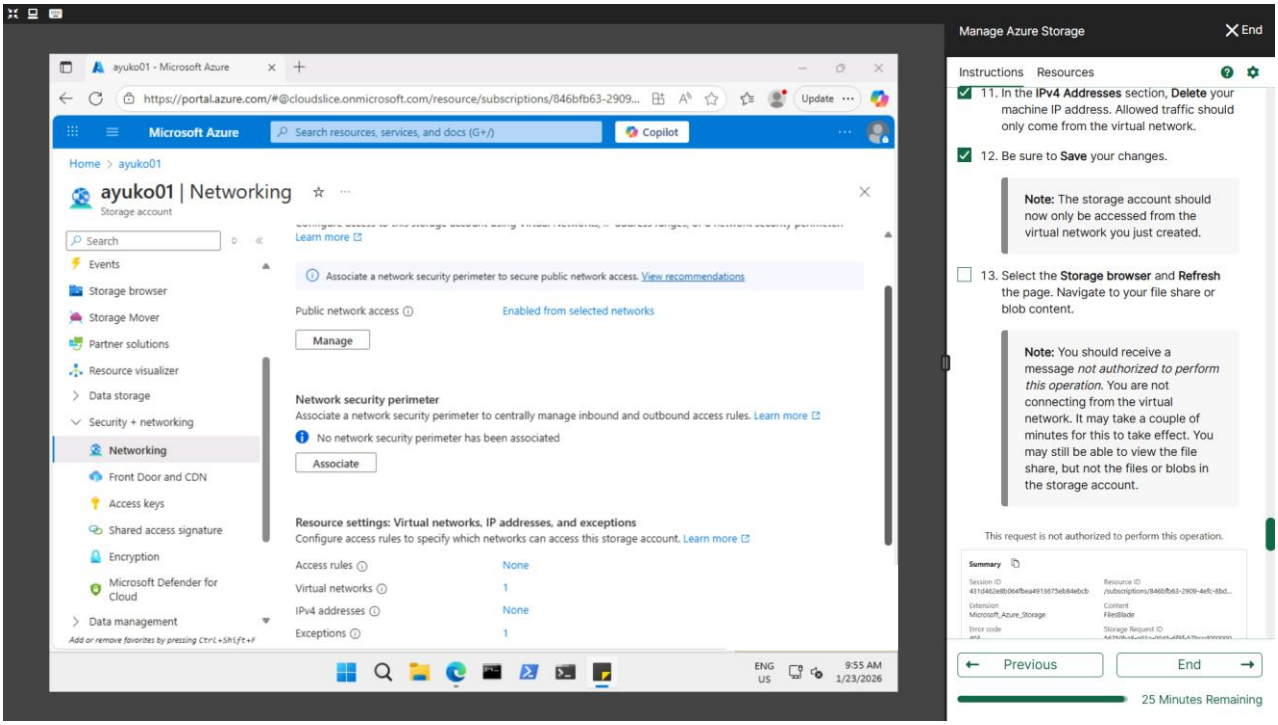


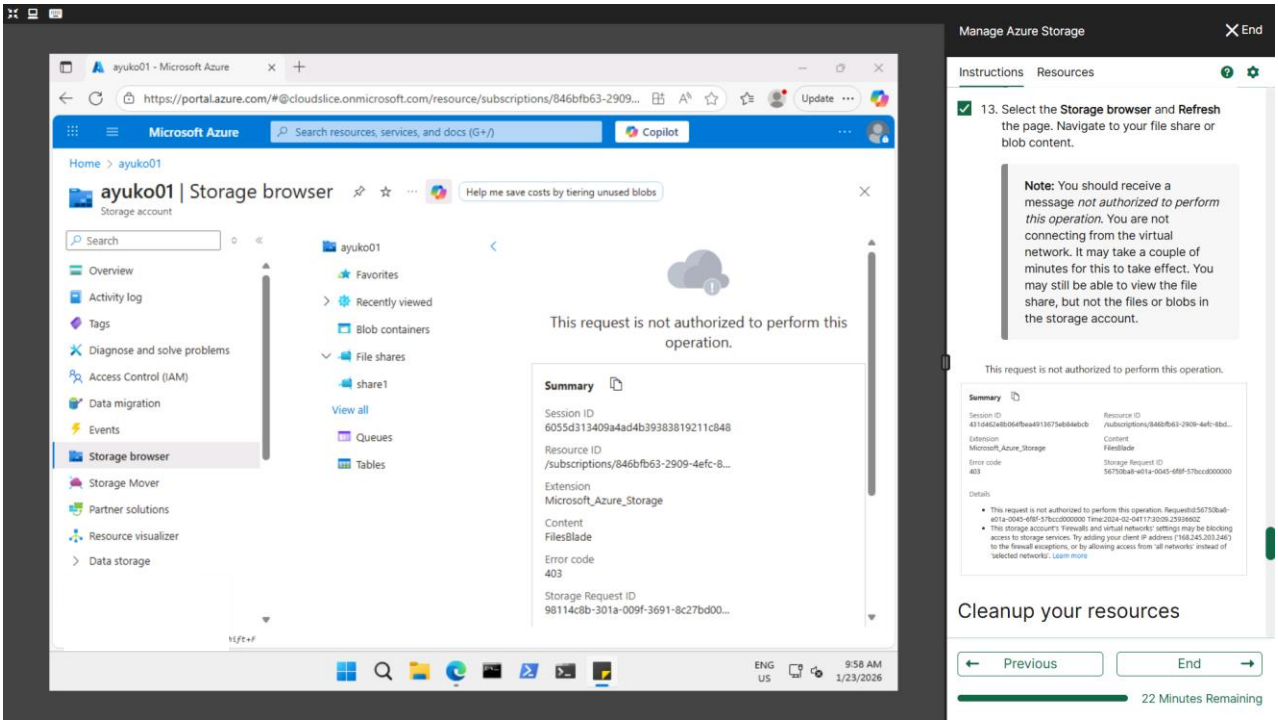
- Network Access Restrictions for Storage Accounts




vnet1 - Microsoft Azure
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
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
Filter service endpoints
Service
Subnet
Status
Locations
Microsoft.Storage
1
default
Succeeded
East US, West US, West US 3
ENG
US
9:51 AM
1/23/2026
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


Public network access - Microsoft
https://portal.azure.com/#view/Microsoft_Azure_Storage/ConfigurePublicNetworkAccessAndRes...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
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
az104-rg7-lod5...
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
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


ayuko01 - Microsoft Azure
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
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
ENG
US
9:55 AM
1/23/2026
Manage Azure Storage
End
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
Previous
End
25 Minutes Remaining


ayuko01 - Microsoft Azure
https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/846bfb63-2909...
Update
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > ayuko01
ayuko01 | Storage browser
Storage account
Help me save costs by tiering unused blobs
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
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-301a-009f-3691-8c27bd00...
ENG
US
9:58 AM
1/23/2026
Manage Azure Storage
End
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
Cleanup your resources
Previous
End
22 Minutes Remaining