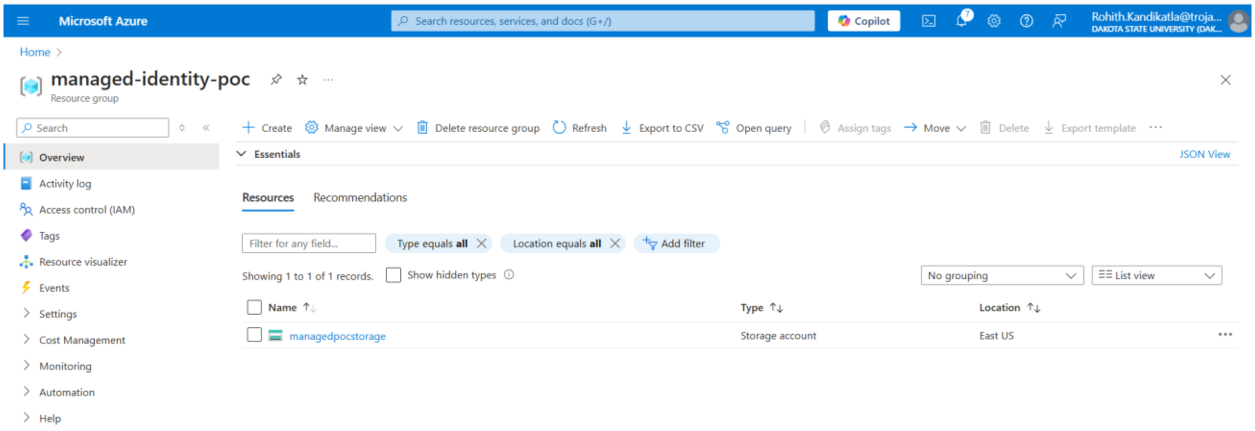
Accessing one resource from another resource using IAM called Managed Identity

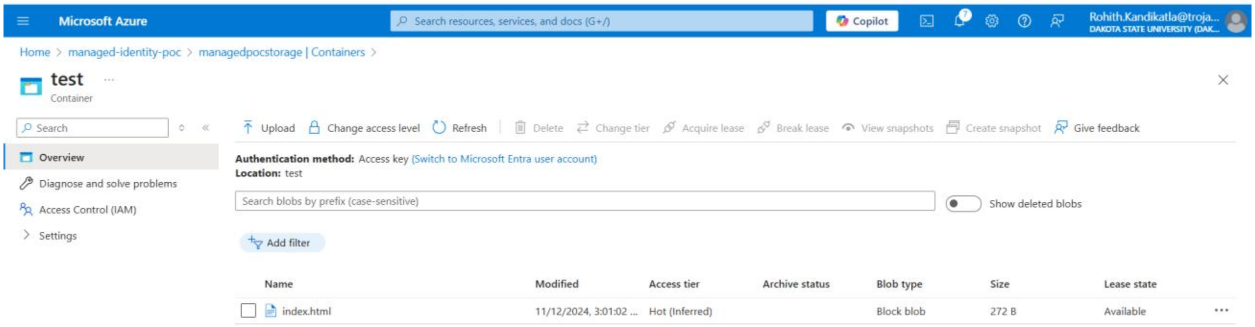
1. Created a resource group



Showing 1 to 1 of 1 records. □ Show hidden types

	Name	Type	Location
□	managedpocstorage	Storage account	East US

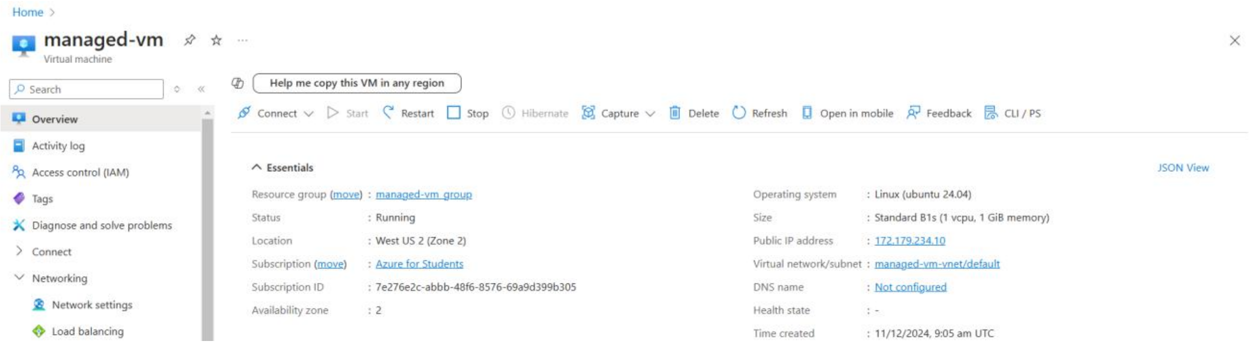
2. Created a storage account and uploaded index.html file


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Rohith.Kandikatla@troja...
DAKOTA STATE UNIVERSITY (DAK...
Home > managed-identity-poc > managedpocstorage | Containers >
test
Container
Search
Overview
Diagnose and solve problems
Access Control (IAM)
Settings
Upload
Change access level
Refresh
Delete
Change tier
Acquire lease
Break lease
View snapshots
Create snapshot
Give feedback
Search blobs by prefix (case-sensitive)
Show deleted blobs
Add filter

Authentication method: Access key (Switch to Microsoft Entra user account)
Location: test

	Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
□	index.html	11/12/2024, 3:01:02 ...	Hot (Inferred)		Block blob	272 B	Available

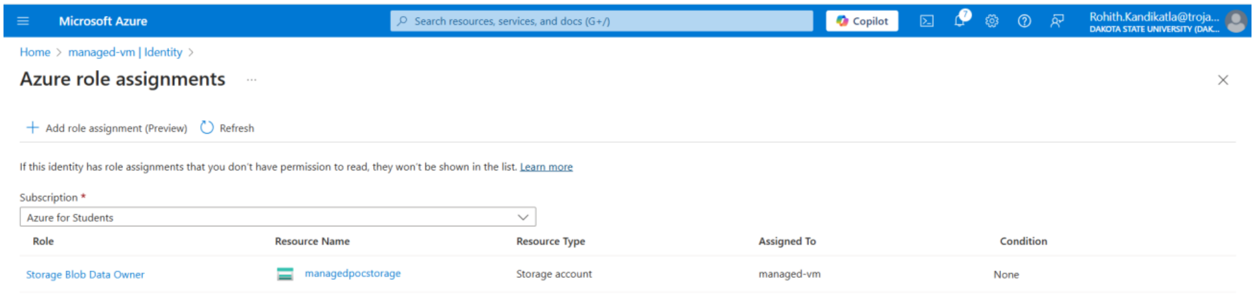
3. Created a VM



Resource group (move) : managed-vm_group
Status : Running
Location : West US 2 (Zone 2)
Subscription (move) : Azure for Students
Subscription ID : 7e276e2c-abbb-48f6-8576-69a9d399b305
Availability zone : 2

Operating system : Linux (ubuntu 24.04)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 172.179.234.10
Virtual network/subnet : managed-vm-vnet/default
DNS name : Not configured
Health state : -
Time created : 11/12/2024, 9:05 am UTC

4. Assigned a role as a identity for storage account to VM


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Rohith.Kandikatla@troja...
DAKOTA STATE UNIVERSITY (DAK...
Home > managed-vm | Identity >
Add role assignment (Preview)
Refresh

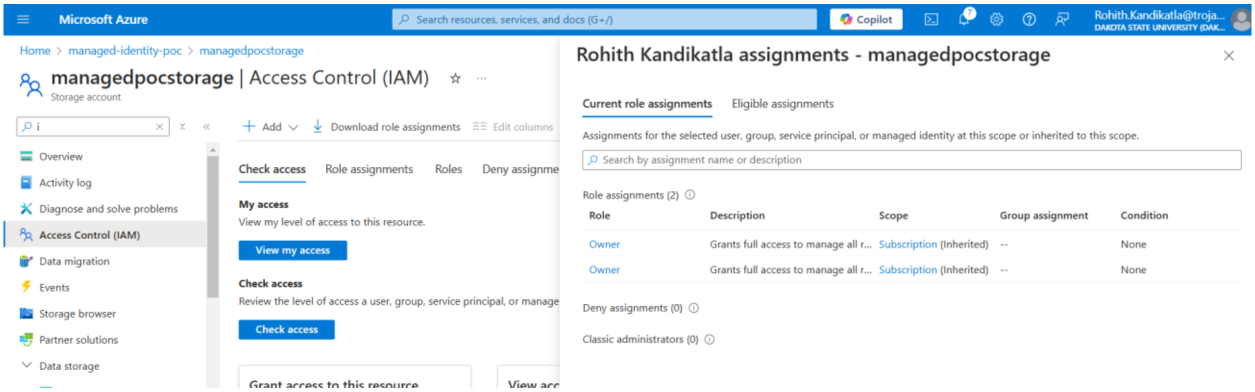
Azure role assignments

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *: Azure for Students

Role	Resource Name	Resource Type	Assigned To	Condition
Storage Blob Data Owner	managedpocstorage	Storage account	managed-vm	None

5. Given owner access of storage account


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Rohith.Kandikatla@troja...
DAKOTA STATE UNIVERSITY (DAK...
Home > managed-identity-poc > managedpocstorage
managedpocstorage | Access Control (IAM)
Storage account
Overview
Activity log
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Partner solutions
Data storage
Add
Download role assignments
Edit columns
Check access
Role assignments
Roles
Deny assignme
My access
View my level of access to this resource.
View my access
Check access
Review the level of access a user, group, service principal, or manage
Check access
Grant access to this resource
View acc

Rohith Kandikatla assignments - managedpocstorage

Current role assignments | Eligible assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

Search by assignment name or description

Role assignments (2)

Role	Description	Scope	Group assignment	Condition
Owner	Grants full access to manage all r...	Subscription (Inherited)	--	None
Owner	Grants full access to manage all r...	Subscription (Inherited)	--	None

Deny assignments (0)

Classic administrators (0)

6. Commands to access Blob from the Virtual Machine

Fetch the access token

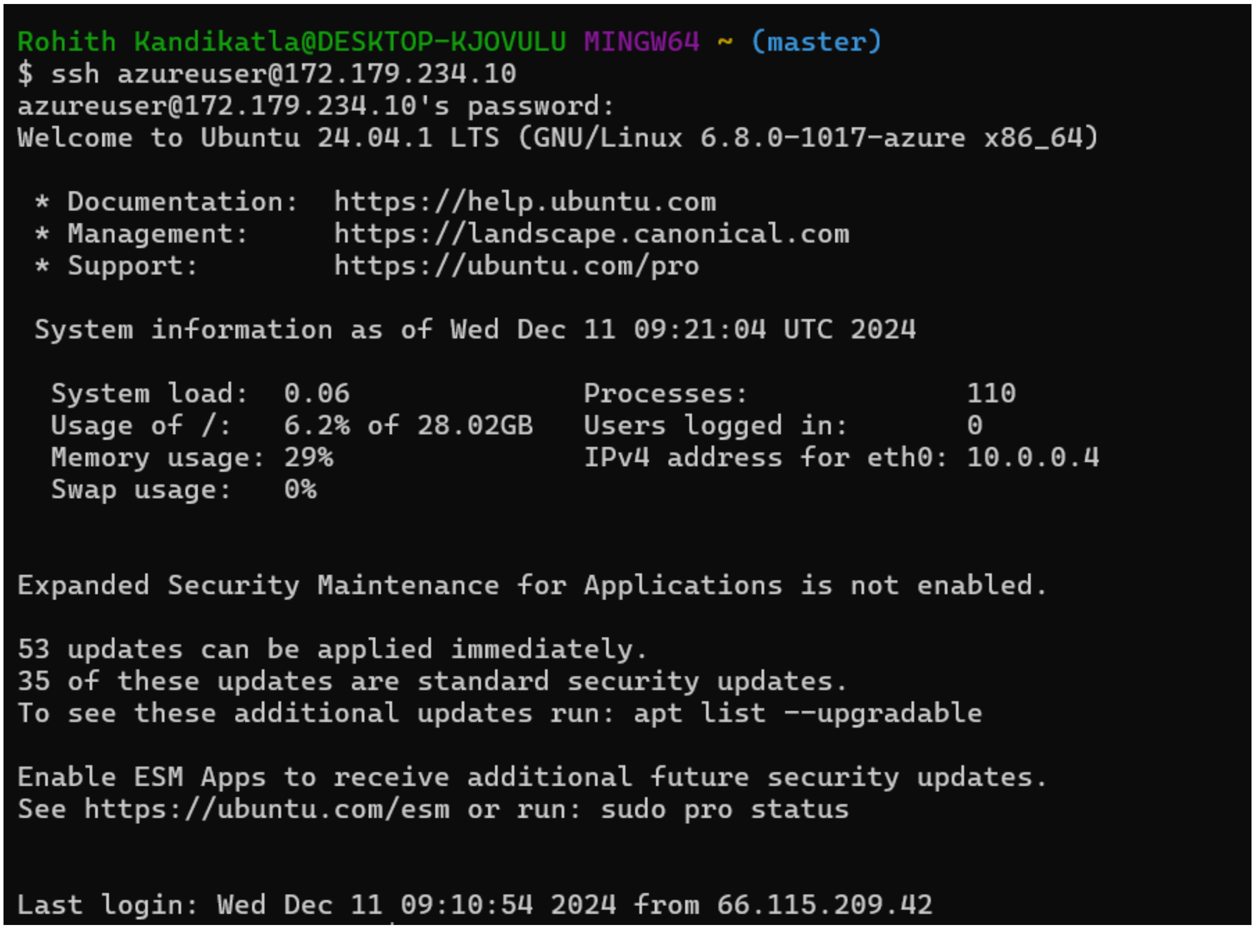
```
access_token=$(curl 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fstorage.azure.com%2F' -H Metadata:true | jq -r '.access_token')
```

Access the blob from Virtual Machine

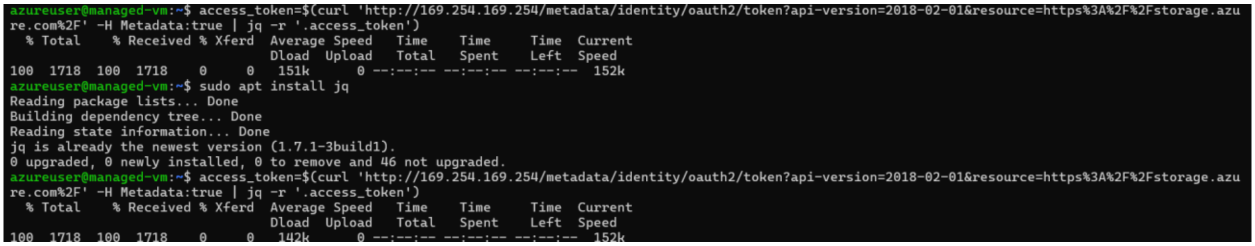
```
storage_account_name="" container_name="" blob_name=""
```

```
curl "https://$storage_account_name.blob.core.windows.net/$container_name/$blob_name" -H "x-ms-version: 2017-11-09" -H "Authorization: Bearer $access_token"
```

7. Logged into VM

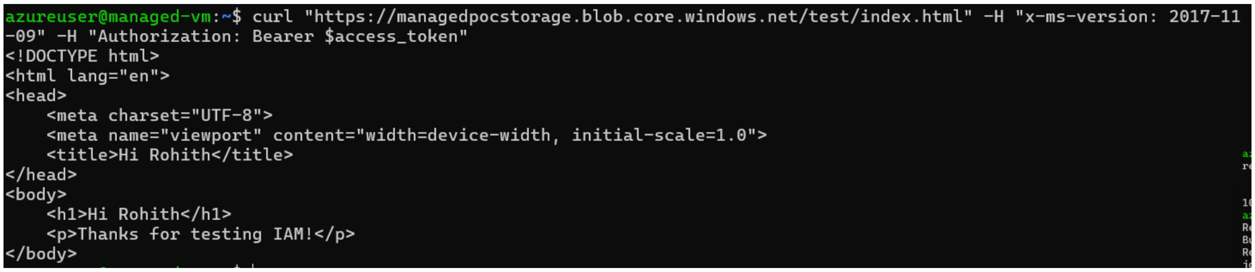


```
Rohith Kandikatla@DESKTOP-KJOVULU MINGW64 ~ (master)
$ ssh azureuser@172.179.234.10
azureuser@172.179.234.10's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1017-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Dec 11 09:21:04 UTC 2024

  System load:  0.06               Processes:             110
  Usage of /:   6.2% of 28.02GB    Users logged in:       0
  Memory usage: 29%                IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

53 updates can be applied immediately.
35 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Wed Dec 11 09:10:54 2024 from 66.115.209.42
```



```
azureuser@managed-vm:~$ access_token=$(curl 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fstorage.azu
re.com%2F' -H Metadata:true | jq -r '.access_token')
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1718  100  1718    0     0   151k      0 --:--:-- --:--:-- --:--:--  152k
azureuser@managed-vm:~$ sudo apt install jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
jq is already the newest version (1.7.1-3build1).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
azureuser@managed-vm:~$ access_token=$(curl 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fstorage.azu
re.com%2F' -H Metadata:true | jq -r '.access_token')
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1718  100  1718    0     0   142k      0 --:--:-- --:--:-- --:--:--  152k
```

8. Accessed the blob from virtual machine



```
azureuser@managed-vm:~$ curl "https://managedpocstorage.blob.core.windows.net/test/index.html" -H "x-ms-version: 2017-11
-09" -H "Authorization: Bearer $access_token"
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Hi Rohith</title>
</head>
<body>
    <h1>Hi Rohith</h1>
    <p>Thanks for testing IAM!</p>
</body>
```