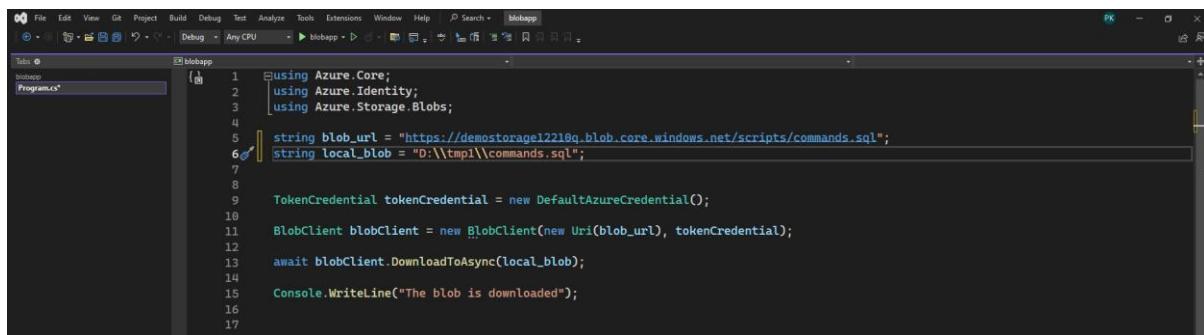




Azure Managed Identity

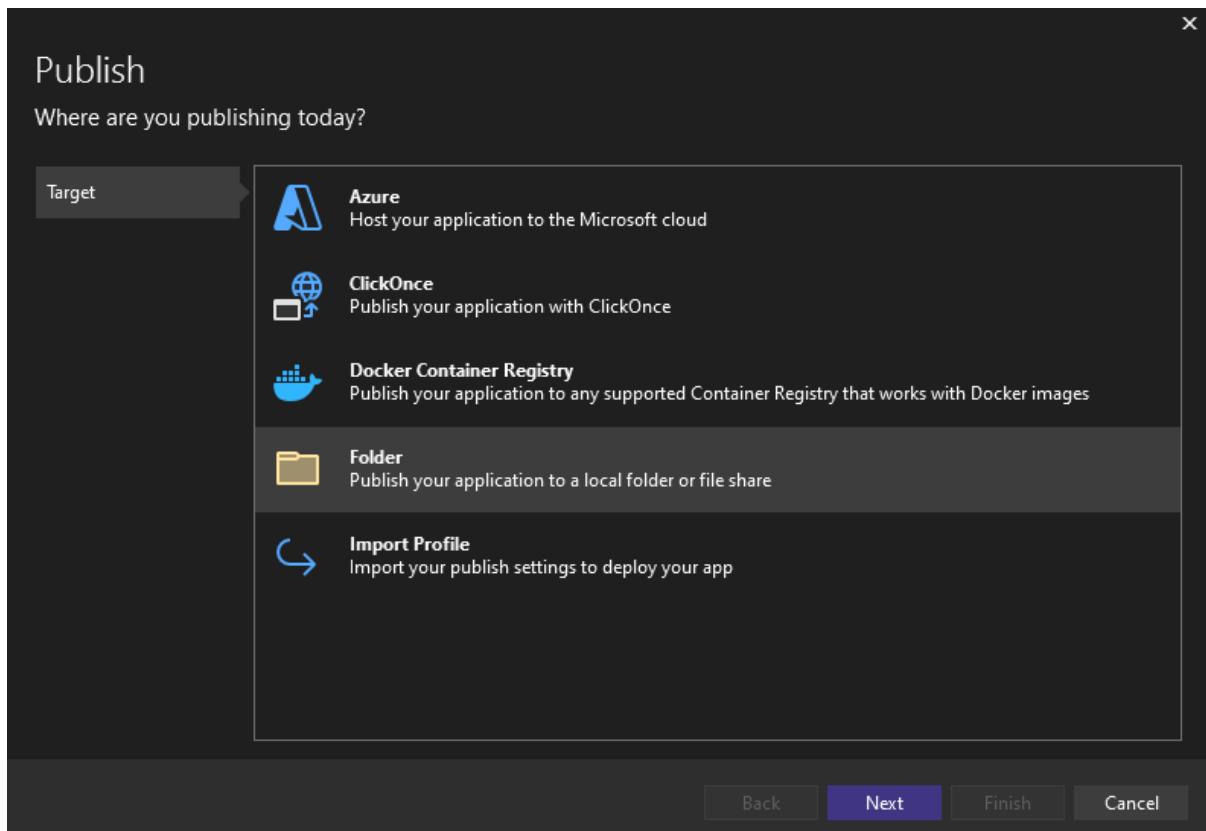
Using a managed identity, we will configure a virtual machine (VM) in this lab to safely access an Azure Storage account and download a file from a container inside the account. The ultimate objective is to demonstrate how managed identities may be used to provide access to Azure resources without requiring manual service principal management or the storage of credentials in code. This makes it easier for administrators to handle identity and access control while ensuring safe and smooth communication between Azure services.

1. In this lab first we need to create a VM based on Windows Server 2022. Then we need to create a Storage account then a container in it.
2. After that we need to put a file on that container. Now we need to download a zip file from GitHub named blob App. Then unzip it and open the application in Microsoft Visual Studio 2022.
3. Below you can see the contents of your application now you need to change something in your blob URL. First, you need to put your storage account name then following through you need to give the container name and then the file name.
4. After that you need to click on build to build the entire solution of your application.

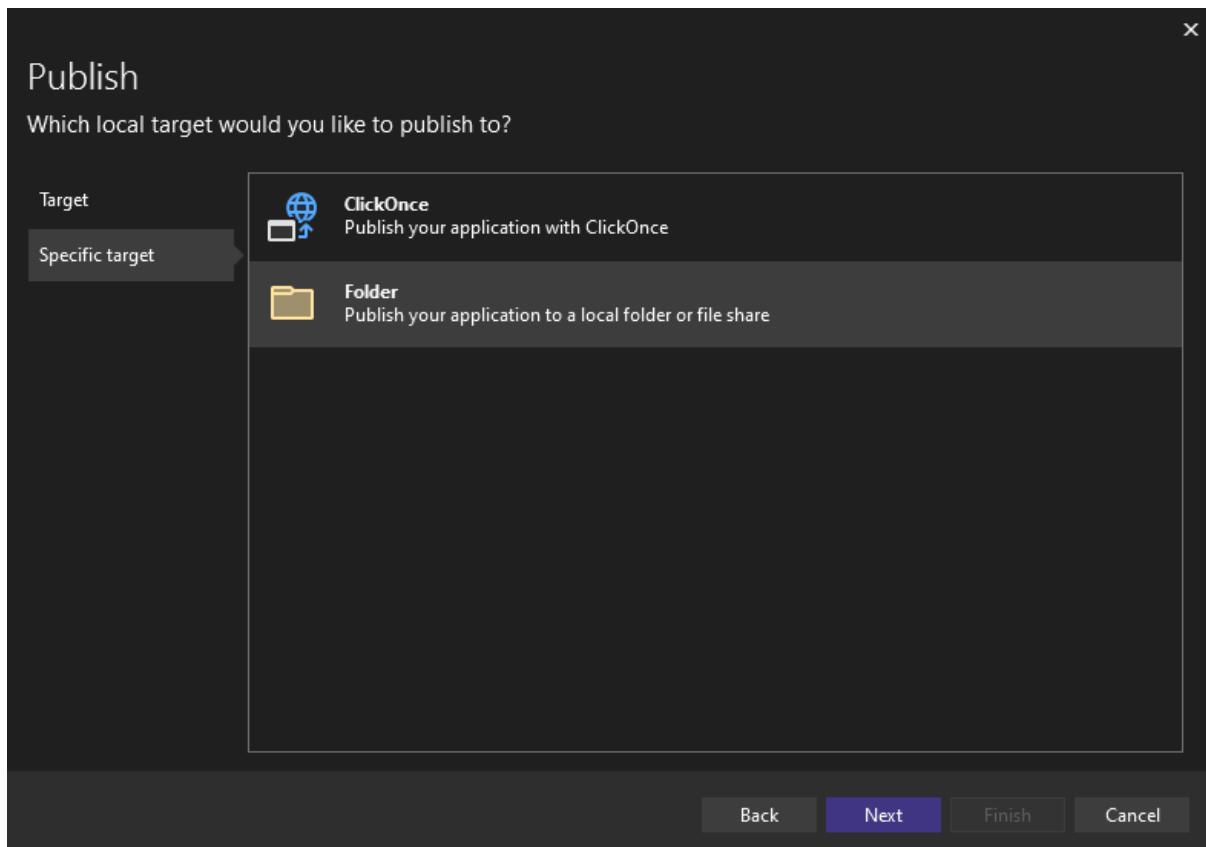


```
blobapp.cs
1  using Azure.Core;
2  using Azure.Identity;
3  using Azure.Storage.Blobs;
4
5  string blob_url = "https://demostorage12210q.blob.core.windows.net/scripts/commands.sql";
6  string local_blob = "D:\\tmp1\\commands.sql";
7
8
9  TokenCredential tokenCredential = new DefaultAzureCredential();
10
11 BlobClient blobClient = new BlobClient(new Uri(blob_url), tokenCredential);
12
13 await blobClient.DownloadToAsync(local_blob);
14
15 Console.WriteLine("The blob is downloaded");
16
17
```

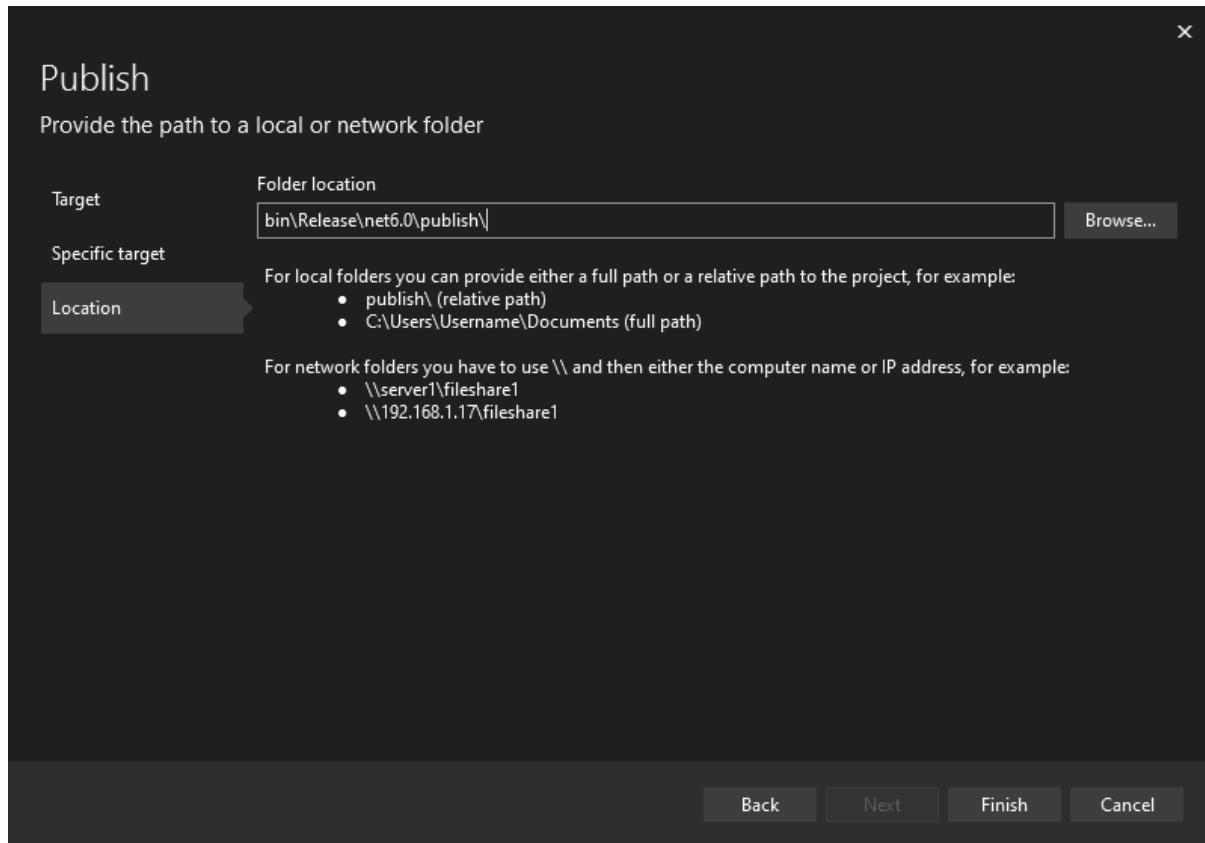
5. Once the build is done then you need to publish this build to a local folder in your laptop. To do that you need to go to the solution explorer and right click on the blobapp and then choose to publish. Then you have to choose folder as shown below.



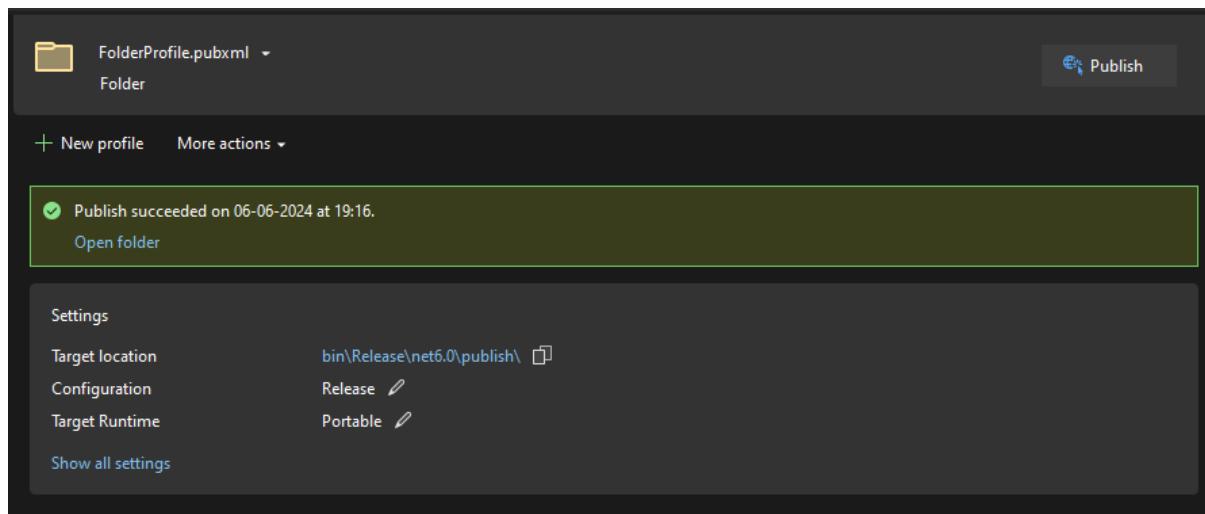
6. After that again choose folder.



7. Here you can see the location of your publish. You can also change the location as per your wish. Then just click on finish.



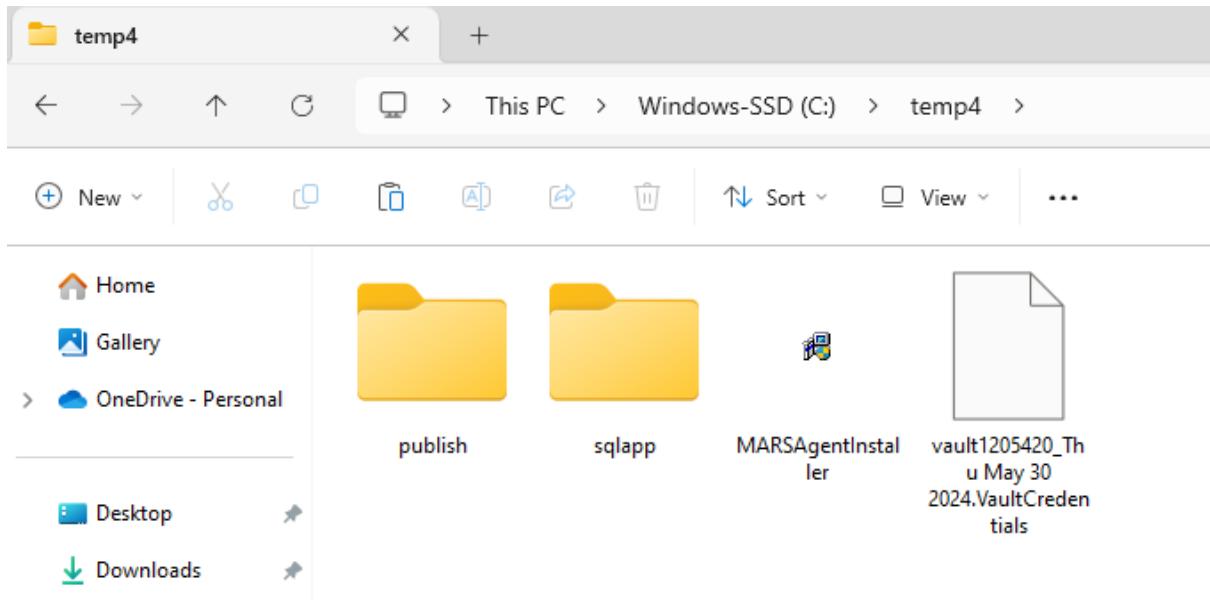
8. Below you can see that we have successfully published it.



9. Here you can see that we are at the location where we have published our application.
10. Now we will copy this publish folder and save in a temporary folder in our C drive on our laptop.

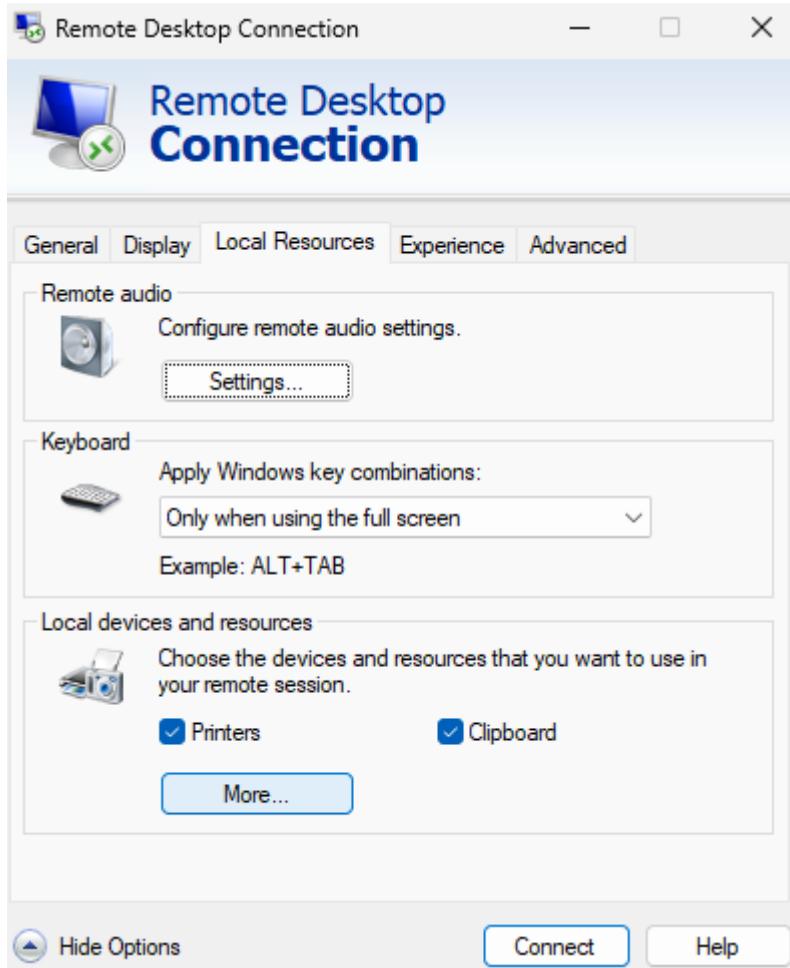
Name	Date modified	Type	Size
Today			
blobapp.deps	06-06-2024 19:16	JSON Source File	13 KB
blobapp.dll	06-06-2024 19:16	Application exten...	6 KB
blobapp	06-06-2024 19:16	Application	146 KB
blobapp.pdb	06-06-2024 19:16	Program Debug D...	11 KB
blobapp.runtimeconfig	06-06-2024 19:16	JSON Source File	1 KB
runtimes	06-06-2024 19:16	File folder	
A long time ago			
Azure.Identity.dll	12-05-2023 03:04	Application exten...	321 KB
Azure.Core.dll	10-05-2023 20:43	Application exten...	328 KB
Azure.Storage.Blobs.dll	11-04-2023 23:15	Application exten...	1,249 KB
Azure.Storage.Common.dll	11-04-2023 23:15	Application exten...	173 KB
Microsoft.Identity.Client.Extensions.Msal...	20-12-2022 11:17	Application exten...	66 KB
Microsoft.Identity.Client.dll	20-12-2022 02:45	Application exten...	932 KB
Microsoft.IdentityModel.Abstractions.dll	27-07-2022 08:38	Application exten...	19 KB
System.IO.Hashing.dll	23-10-2021 05:17	Application exten...	29 KB
System.Memory.Data.dll	08-04-2021 22:15	Application exten...	21 KB
Microsoft.Bcl.AsyncInterfaces.dll	15-04-2020 04:09	Application exten...	15 KB
System.Security.Cryptography.Protected...	15-11-2019 14:07	Application exten...	18 KB

11. You also need to do the same with your publish folder.

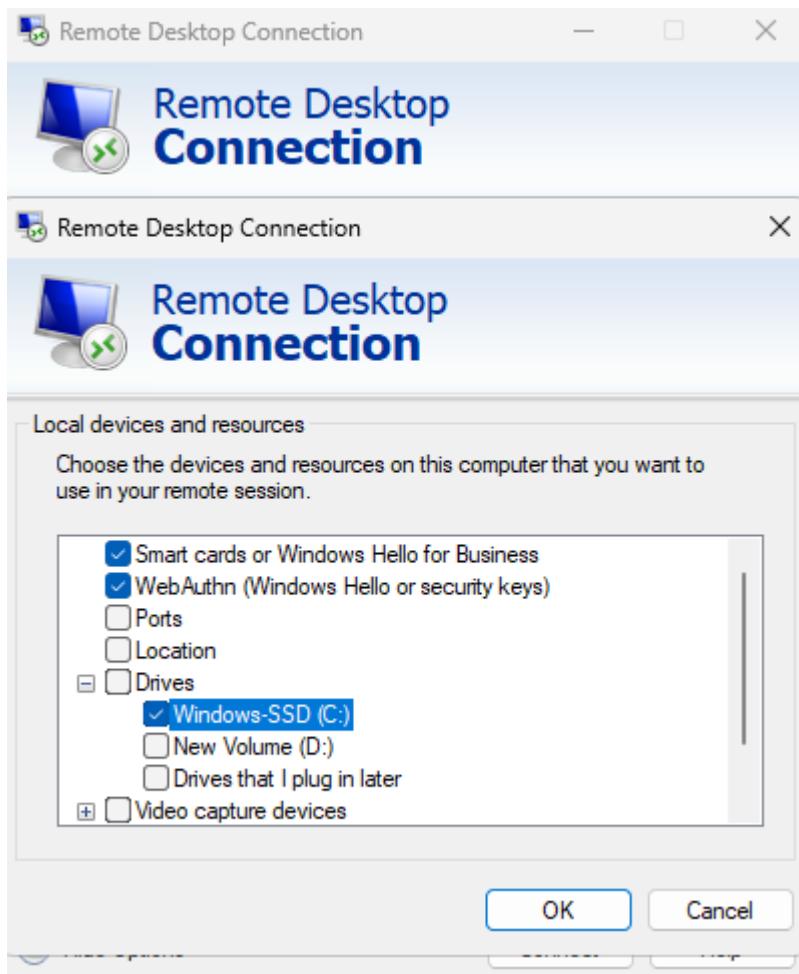


12. After that go back to your Azure Portal and download the RDP file of your VM.

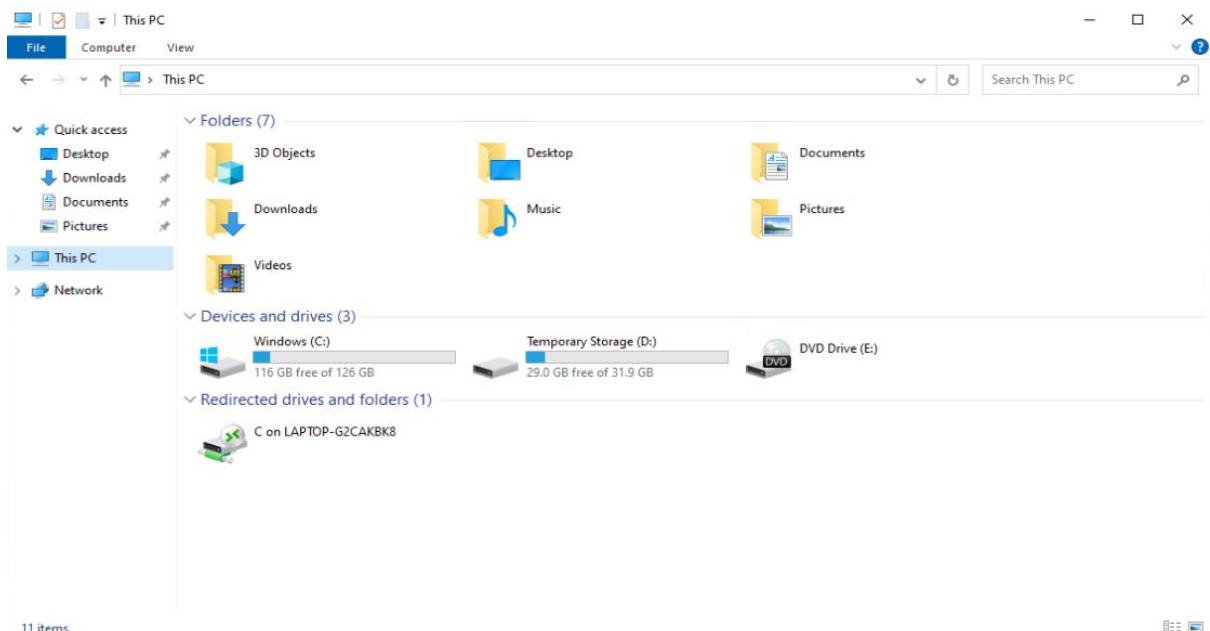
13. Then in your laptop where the RDP file is downloaded, right-click on it and choose to edit it. Then go to local resources and click on more.



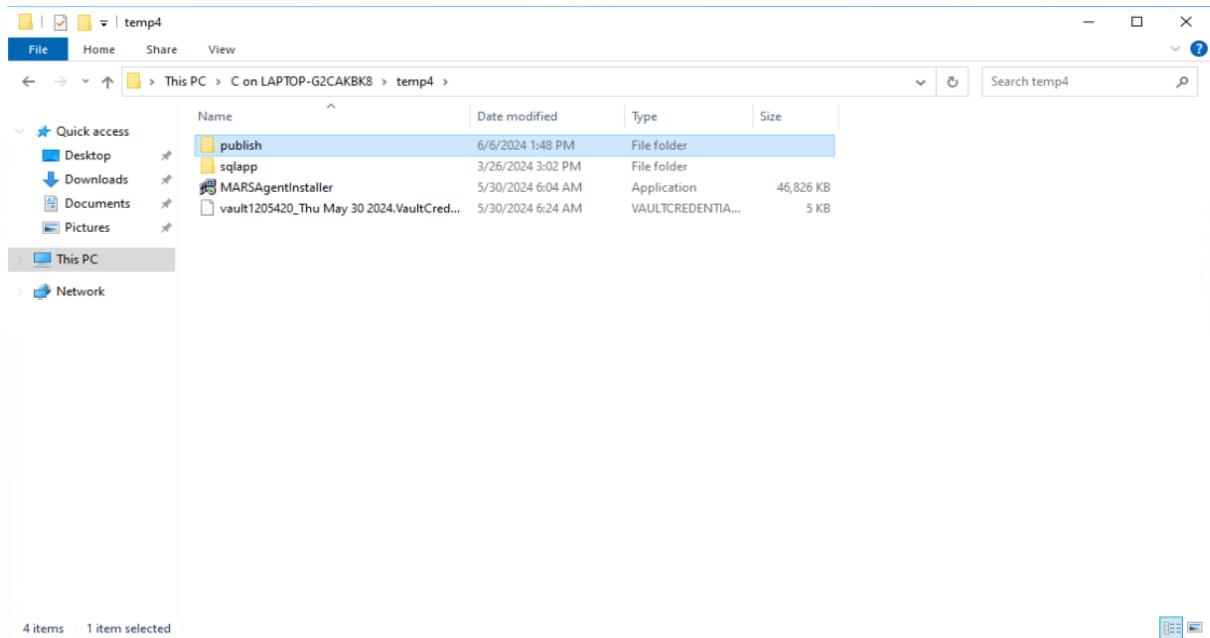
14. Now you need to expand the drives section and choose your C drive or whichever drive that have your publish folder in it. Then click on OK and connect to your VM.



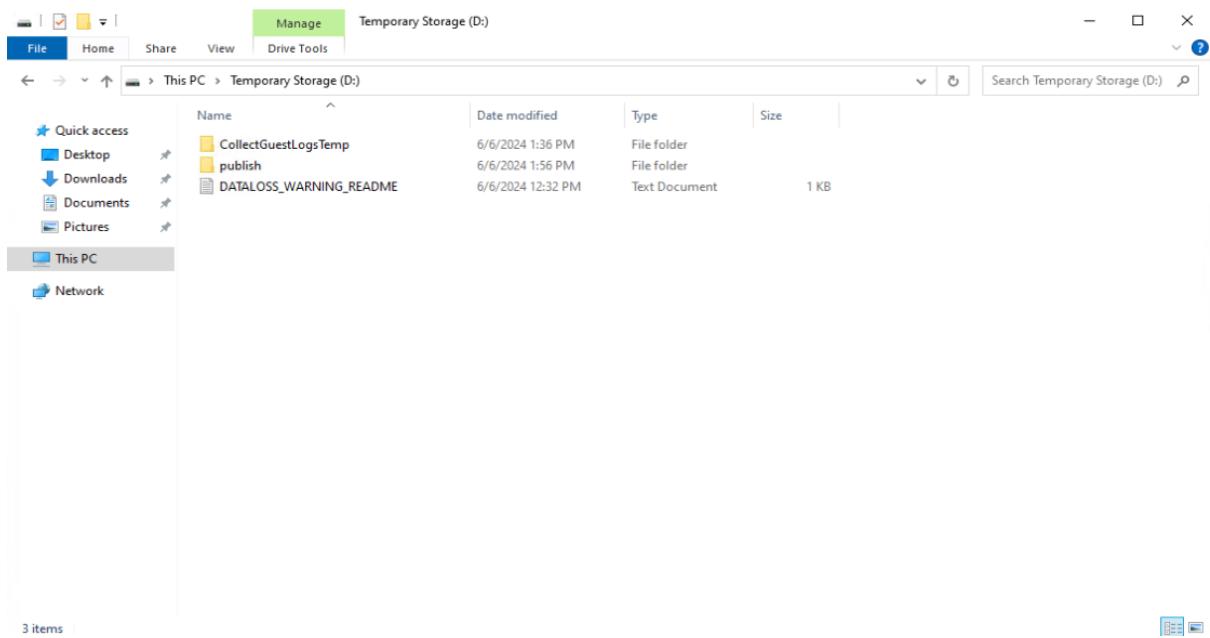
15. Now inside your VM if you go to file explorer and go to This PC, here you will see that you can access then C drive of your Laptop in your VM.



16. Then go to the temp folder in the C drive and copy the Publish folder and paste it in the D drive of your VM.



17. Below you can see that the publish folder has been copied to D drive of our VM successfully.



18. Now in your Azure Portal go to your VM then go to identity, if you see that system assigned identity status is off you need to turn it on. By enabling this feature, we are saying that our VM is now a part of Microsoft Entra ID.

19. Below you can see that it is now turned on. Now we need to give the appropriate permissions.

20. For that you need to go to your Azure Storage account and go to IAM then you need to add a role assignment and choose **Reader role** and in the members you need to add your VM. Then just assign this role.

21. Again, we need to add another role assignment in the same way and choose the role **Storage blob data reader** then you need to choose your VM as your member.

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

X Type : All Category : All

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Defender for Storage Data Scanner	Grants access to read blobs and update index tags. This role is used by the data scanner of Defender for Storage.	BuiltinRole	None	View
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltinRole	Storage	View
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltinRole	Storage	View
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltinRole	Storage	View
Storage Blob Delegator	Allows for generation of a user delegation key which can be used to sign SAS tokens	BuiltinRole	Storage	View

Showing 1 - 5 of 5 results.

Add role assignment ...

Role Members Conditions Review + assign

Selected role Reader

Assign access to User, group, or service principal Managed identity

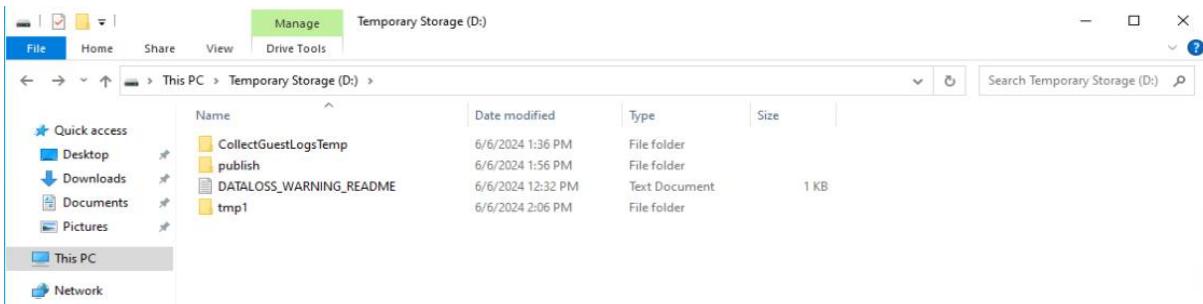
Members [+ Select members](#)

Name	Object ID	Type
No members selected		

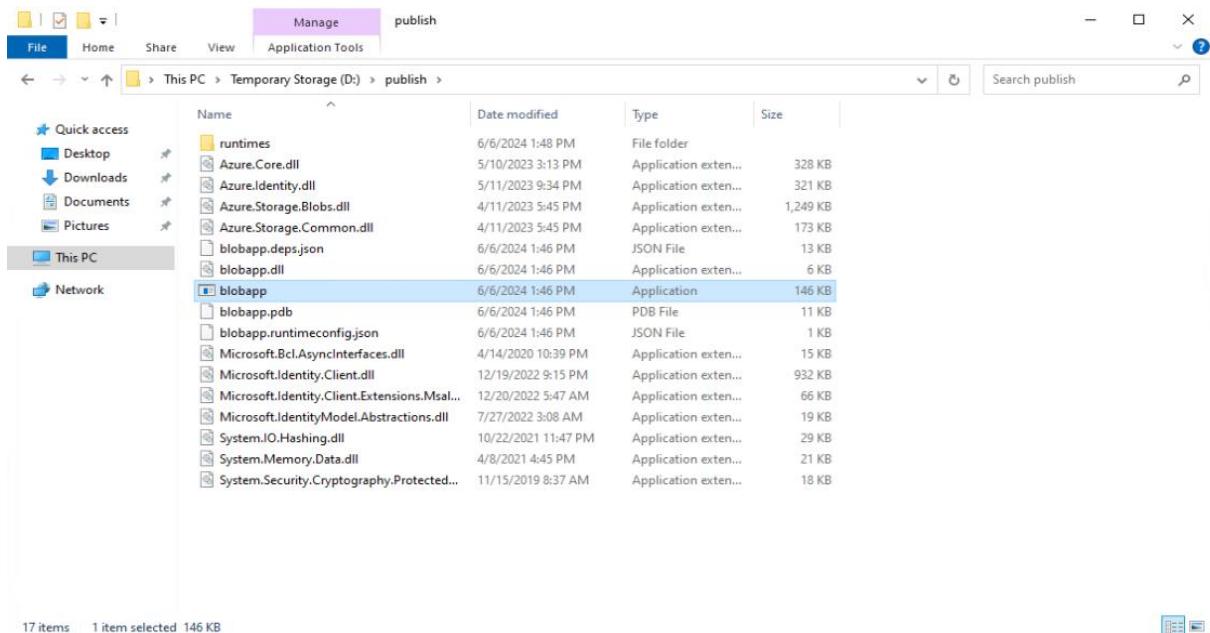
Description

[Review + assign](#) [Previous](#) [Next](#) [Select](#) [Close](#)

22. After that go back to your VM and in your D drive create a folder with the name tmp1.



23. Then you need to go to publish folder and double click on the blob app to run your application.



24. And then if you go to tmp1 folder you will see that file in place.

