**Day -12 | Azure IAM from Basics | Azure Managed Identities Demo with Microsoft Entra (With Notes)**



What is Azure Iam:

**Secure access to your resources with Azure identity and access management solutions. Protect your applications and data at the front gate with Azure identity and access management solutions.**

Two main concepts:

Authenctication

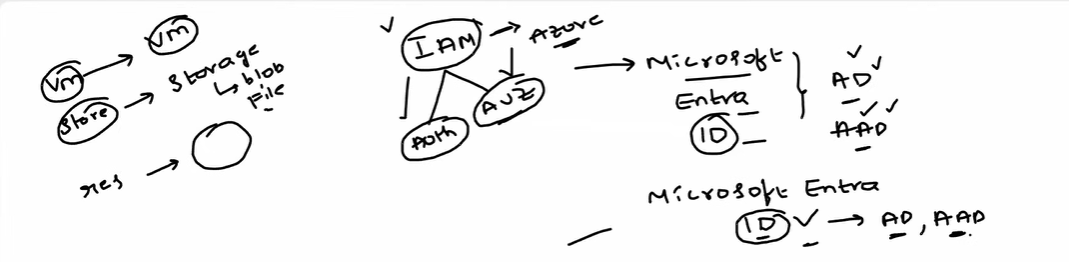
Authorisation

## Authentication

Authentication is the process of proving that you're who you say you are. This is achieved by verification of the identity of a person or device. It's sometimes shortened to AuthN. The Microsoft identity platform uses the [OpenID Connect](https://openid.net/connect/) protocol for handling authentication.

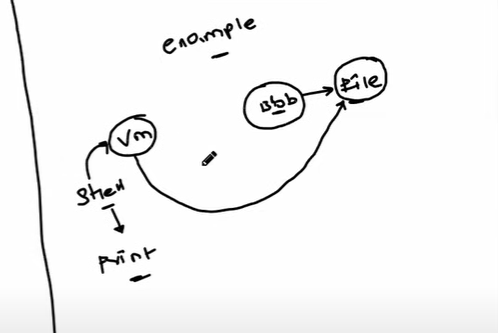
## Authorization

Authorization is the act of granting an authenticated party permission to do something. It specifies what data you're allowed to access and what you can do with that data. Authorization is sometimes shortened to AuthZ. The Microsoft identity platform uses the [OAuth 2.0](https://oauth.net/2/) protocol for handling authorization.



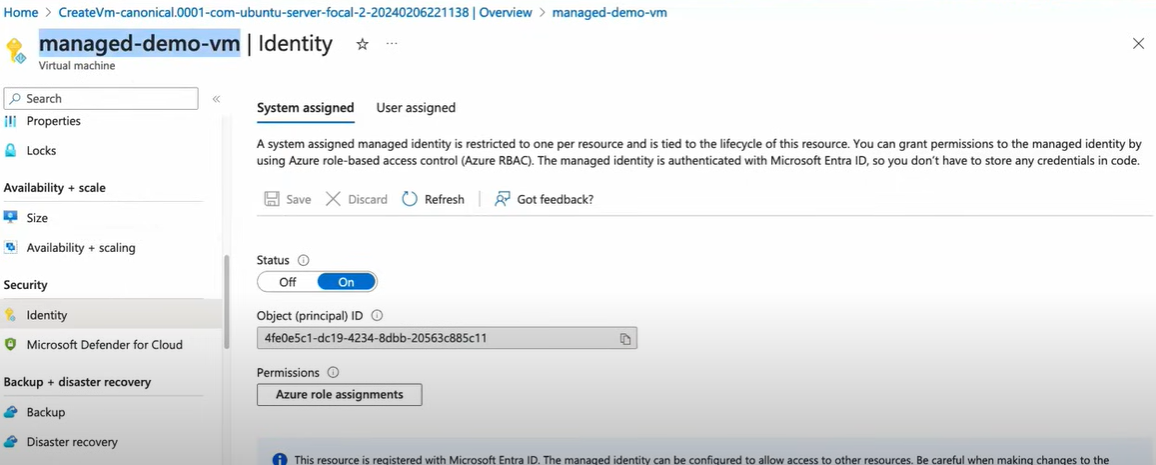
Demo example:

If a developer request an access to the storage account container from their Vm:



Create a storage account aand a VM

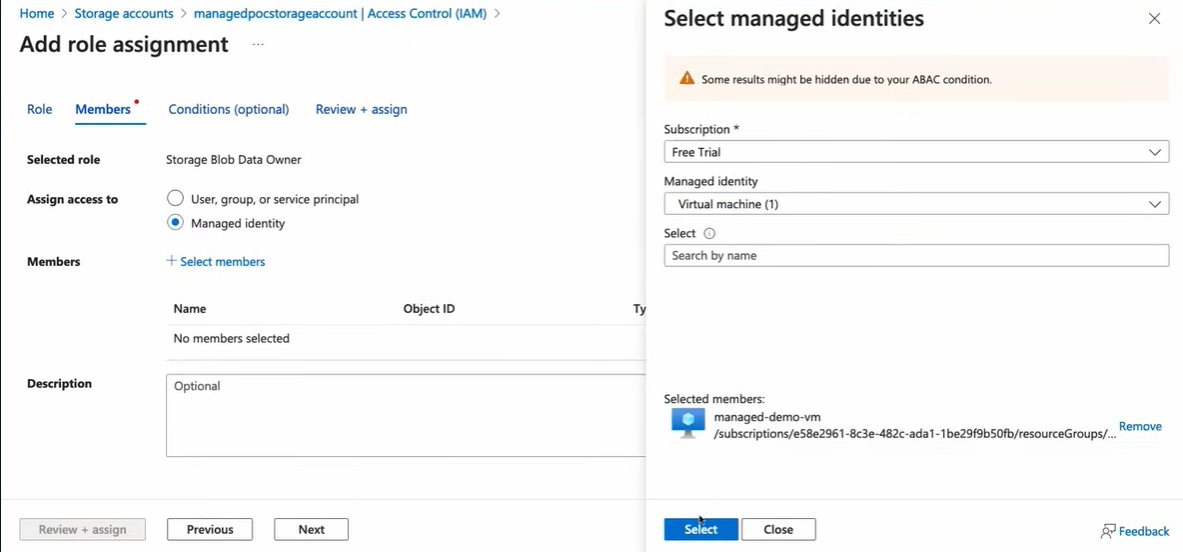
So in VM go in identity and ON the status and save it



Copy the object principal or a VM name.

Then:

Go in storage account 🡪 access IAM🡪add role assignment🡪 search for the role you want(in our case we will give owner access to storage account)



The role is given and you have given the access.

To test:

Open a Vm you have created by SSH

Ssh azureuser@IP

Sudo apt update

Suod apt update jq

### 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')

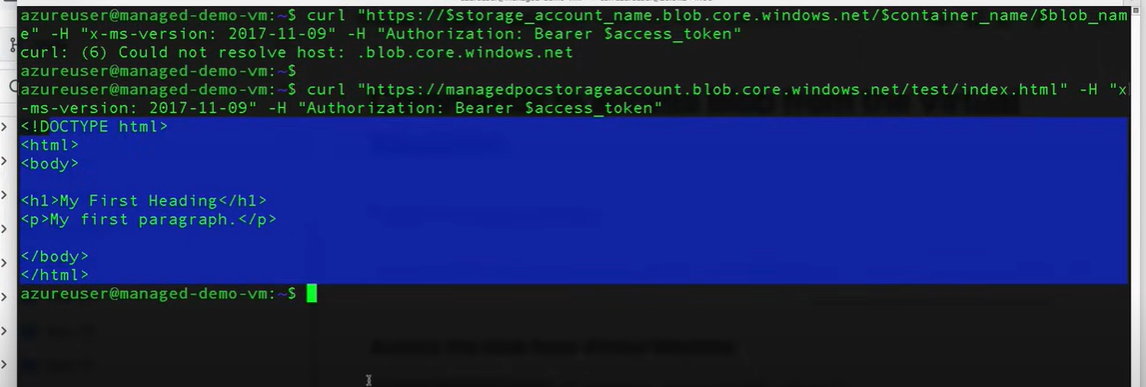
### Access the blob from Virtual Machine

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"

give the storage account name : that you gave for it

container name

blob name:



Once you run this command your Vm is able to access the blob storage files and other things.

So the access is granted succsfully to the VM.

[**https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management**](https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management)

[**https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization**](https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization)