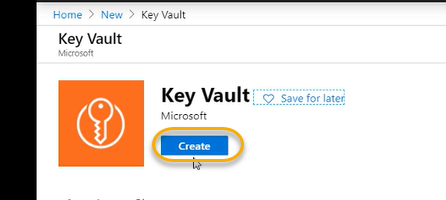
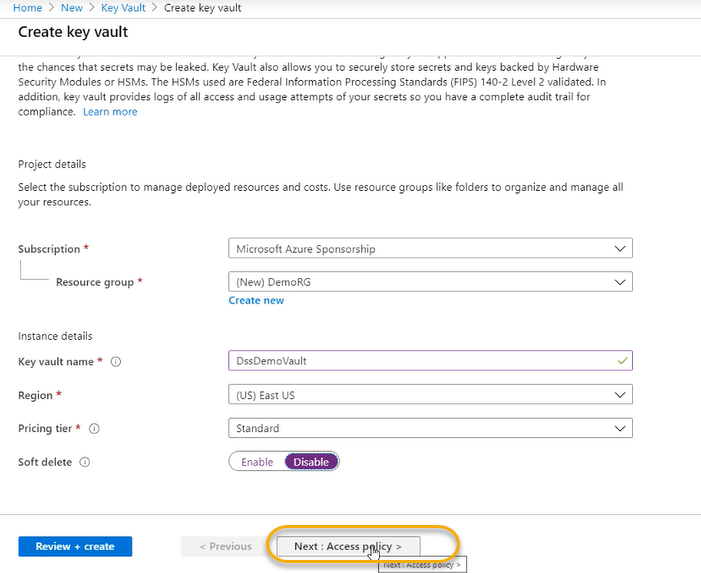
Azure key Vault

1. Let we have data developer profile, tester profile, devOps Profile we have knowledge of Azure Key Vault is essential for everyone
2. Because this is where everyone is going to secure the files
3. Connection to database we need connection strings. Any kind of secure data we would like to manage and the best way we can manage is key vault
4. Key vault is a like a bank locker where we can store Gold and like stuff
5. In Key Vault there are more protocols implemented which is going to make it almost impossible for a hacker to hack vault and extract the data from it
6. We will keep cryptographic keys, certificates, and secrets
7. Certificates are PFX files CRS files
8. A secret is not only text data even it is a binary data. Maximum secret value is 10KB in size and I Can store password as my storage. I can store connection string to database and key which is responsible for encryption and decryption we can store it.
9. We can store it and retrieve it and whenever you need to retrieve, we need proper authentication
10. So, I have to authenticate and then I need authorize to retrieve the data
11. Most of the time the reference of the key we give to some other APIS which will use that key to performing encryption and decryption
12. If at all I am storing my data in Azure storage Account I can store it as private container or a public container
13. If I put it as private container no body will be access the content unless they will have authorization/allow to access it
14. If it is public any body who knows the URL we will be able access it and download it
15. The container is public and still we will want that particular container which can be text file and though it can be accessible it should all saved in a encrypted form
16. We got storage API which I will give reference my key and the storage API would use that key for encrypting storing in the storage account and at the same time I will use the same key for retrieving the data from the storage account and decrypting it.
17. We are not going to use that key directly
18. The VM data should be encrypted and can be saved on the disk so even VM is loose no on one can see the data
19. Someone with in Microsoft is trying to steal the data however he cannot do it because key in the key vault which I will alone has access and the reference of the key in the key vault which I was going to give to the O.S which will be able to do encrypt the data only I have given the permission
20. If the VM resources that do not have permission to the key vault, then the VM will not be able to read the key and will not be able to decrypt the data
21. Any instances where the keys are Indirectly used, and we don’t need to know the value whatever the value will be it is all managed my API for encryption and decryption
22. Key vault as service how it will works?
23. Any developer





Access policy:

Key vault is an Azure service which will be managed keys and services. Any user who wants to manage the service needs a contributor role (Role Based accessed controller)/owner/reader

Contributor can only manage and cannot give permissions to others that is only difference between owner and contributor

The keys and secrets present in the key vault are available in the form of URL

To access the key and secrets we are supposed to use

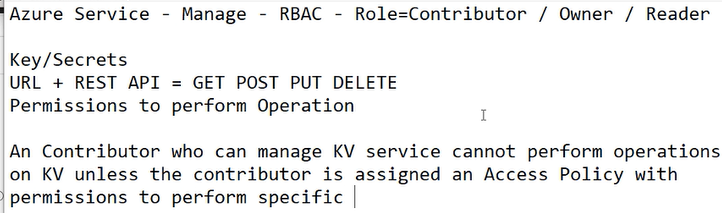
If you want to access the password so in the key vault I will store the secret called password and that is going to have as a URL

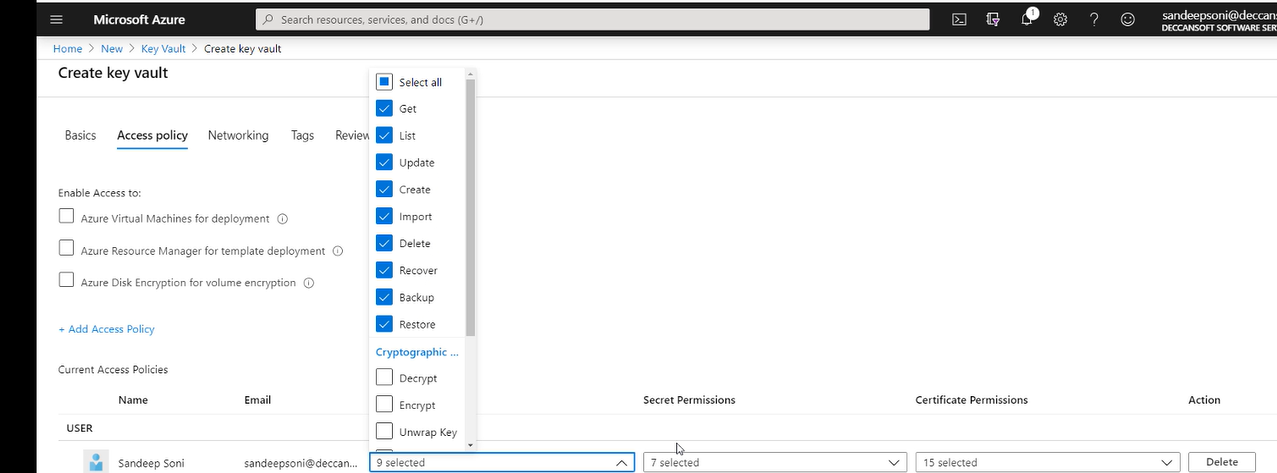
That URL and Rest API is what we will have to use for accessing the secrets

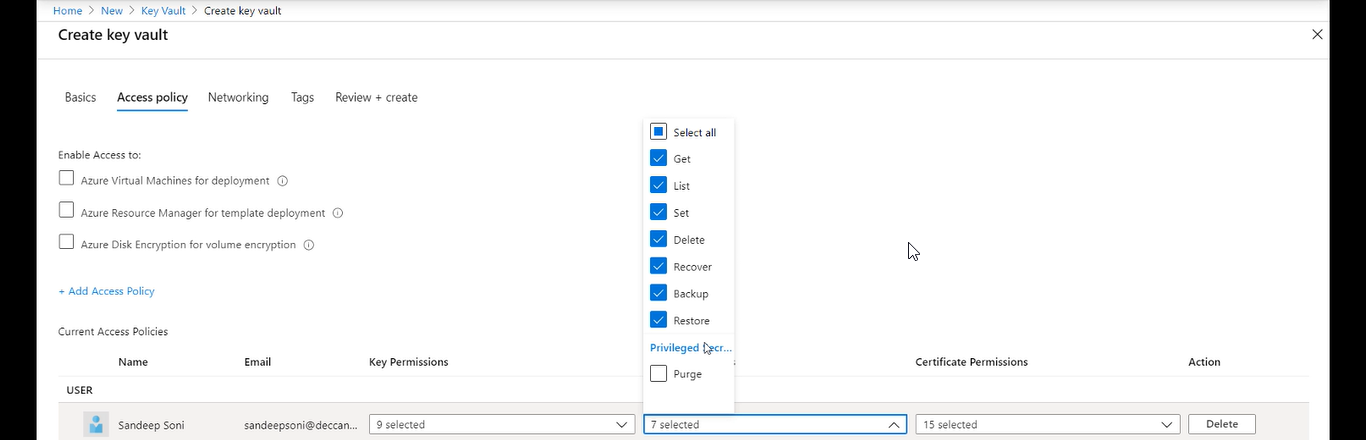
GET, POST, PUT, DELETE ARE http methods

For any body to access keys and vaults they need to have permissions on the operations

A contributor cannot access the key vaults and secrets unless access policy is created for the user



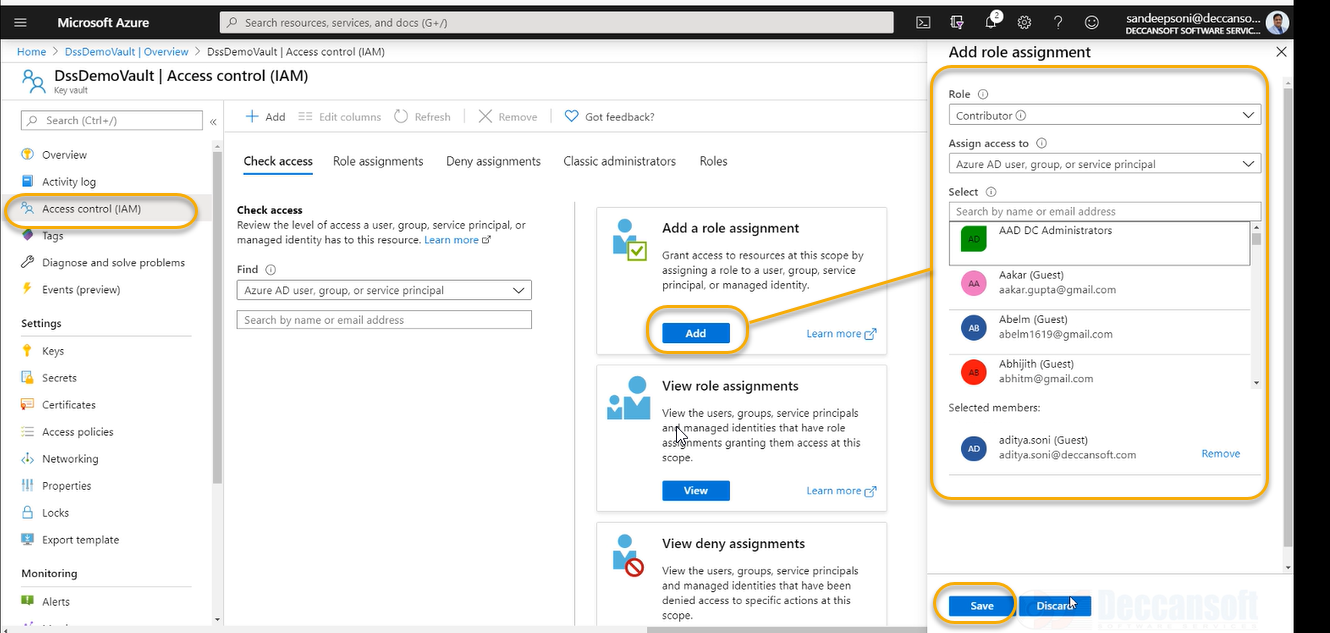






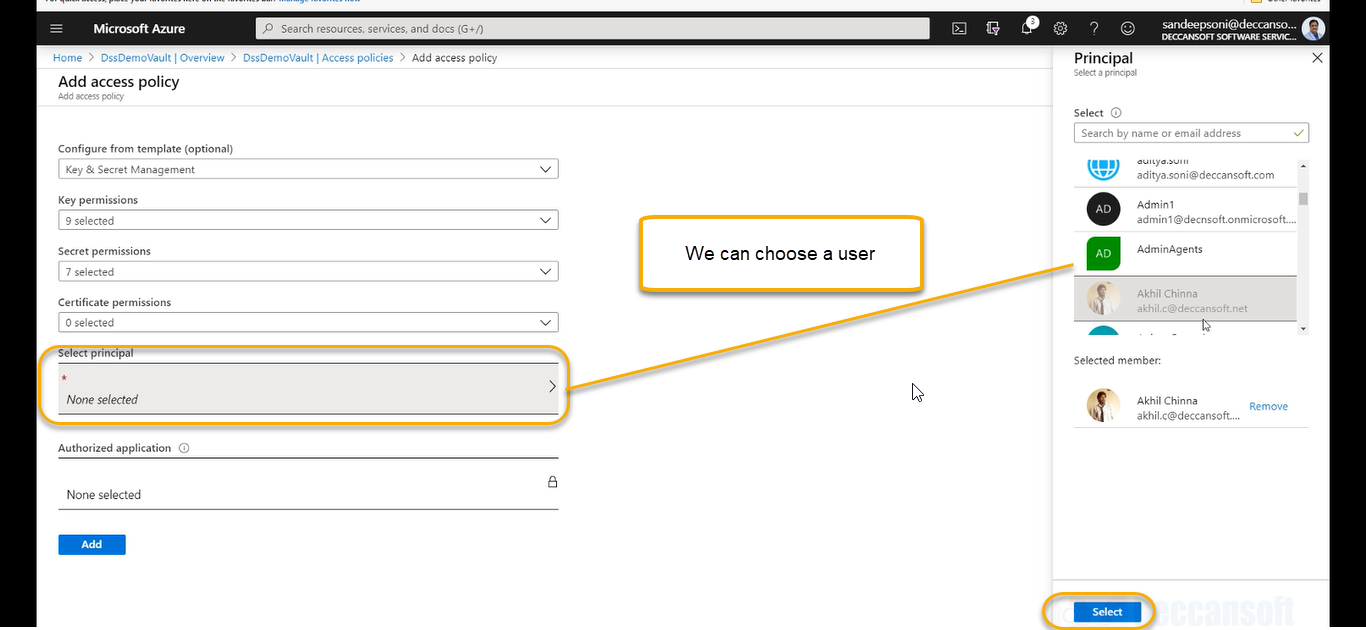
Select the default steps and create the key vault

Now add user to contributor role



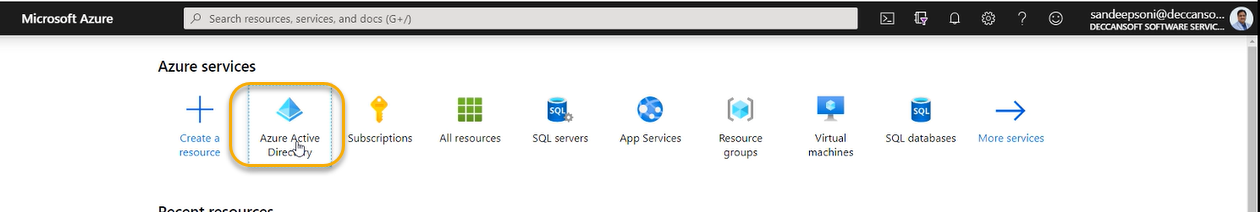
Now the user still NOT accessible to Key Vaults

For that we need to configure the below things



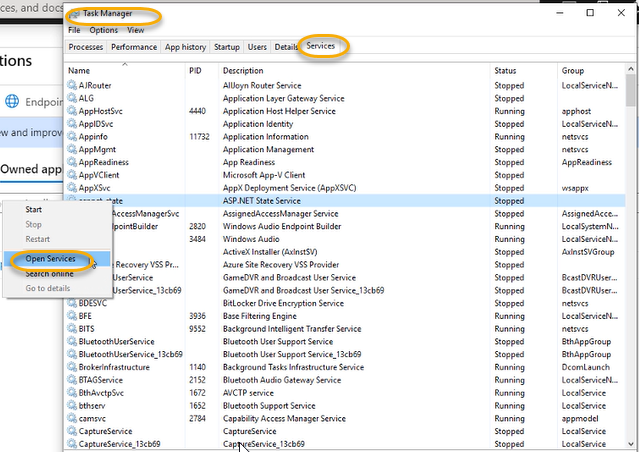
We need to assign that user to Azure AD Application

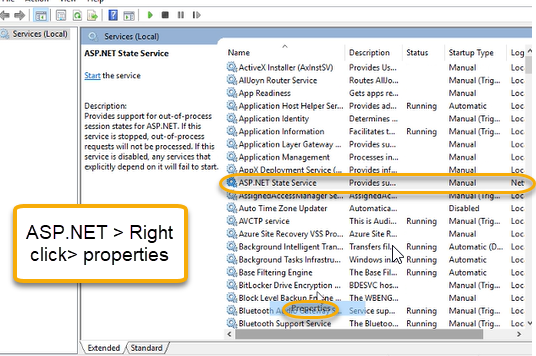
Azure AD Application

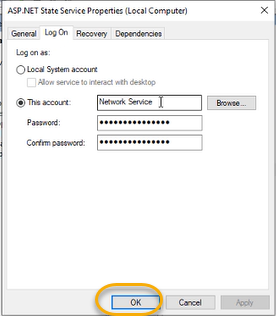


In our machine we have service accounts and those are used to RUN various windows operations which there are along the machine

Some time we need service account for this. Click aspnet\_state > OPEN SERVICES

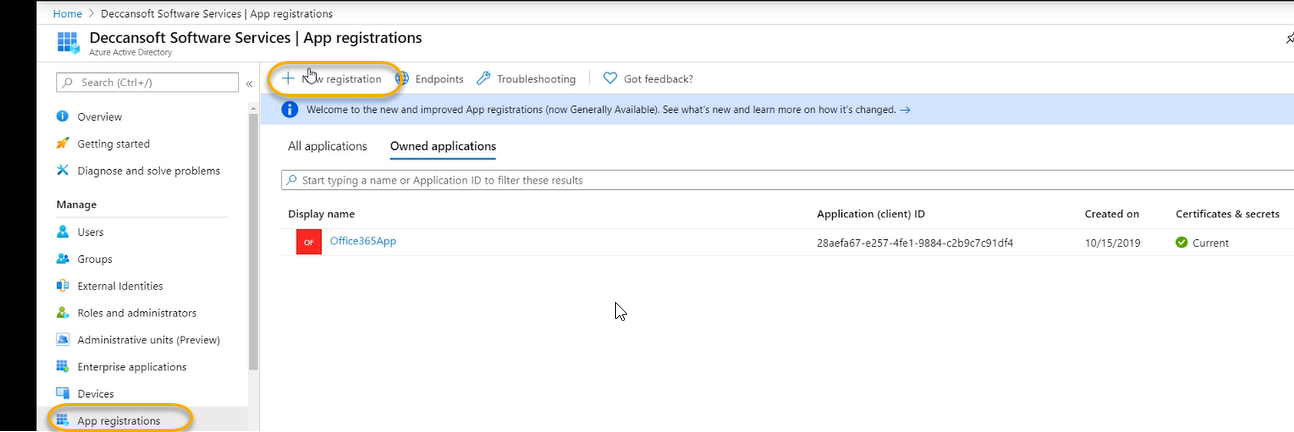


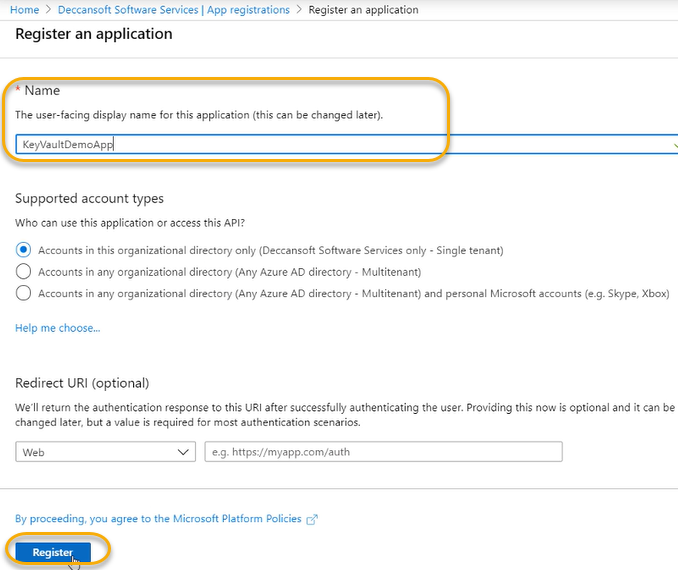




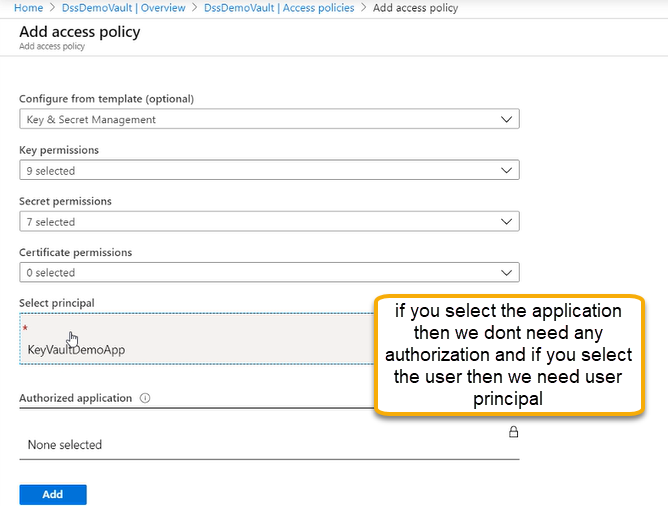
Using the above service this particular account ASP.NET state service is going to access various resources

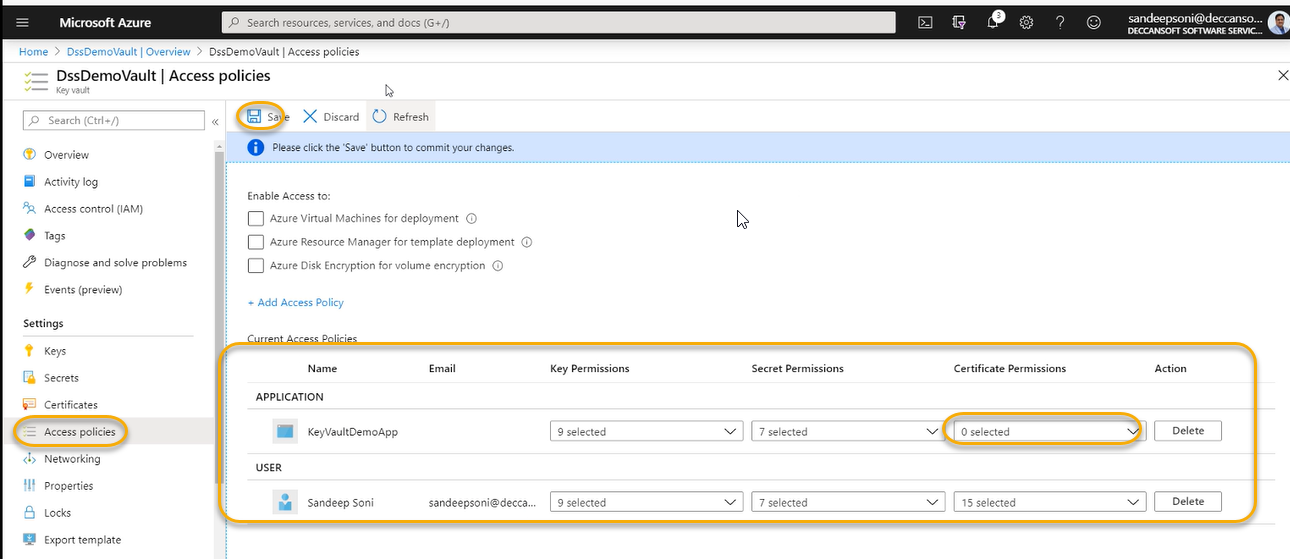
In context of Azure if my application requires to access the certain resources of Azure again the identity can be user and the identity can be for the program and if the program requires the identity it will use the identity of App registrations which is generally referred as service principal





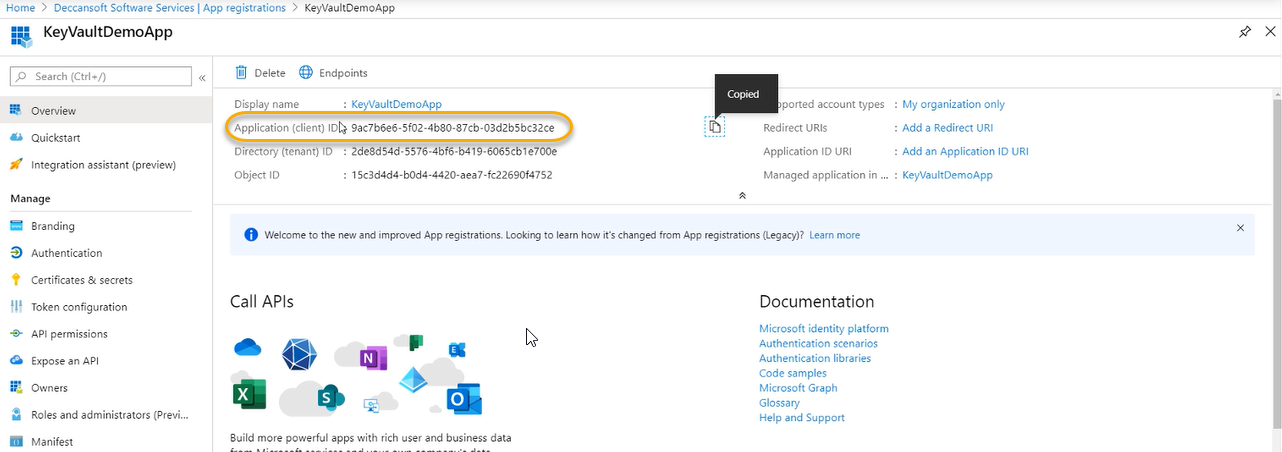
This Azure AD App will now be granted permissions so that program can take the identity of Azure AD App and perform the actions

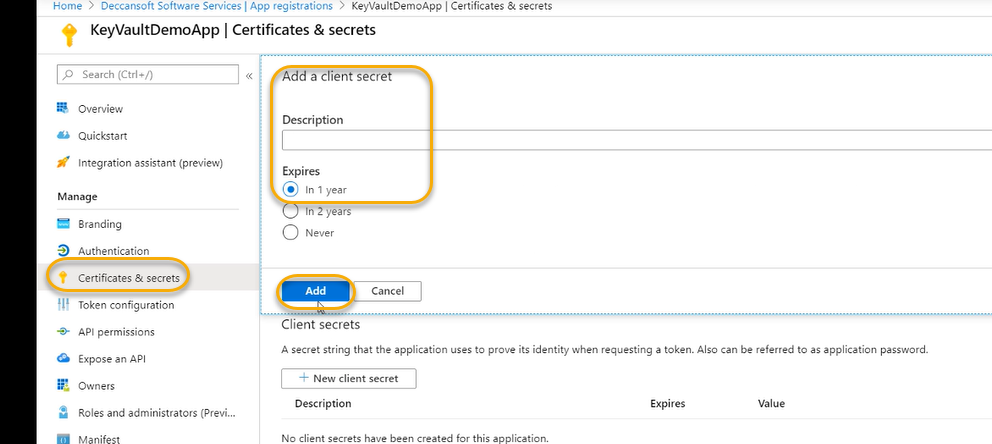


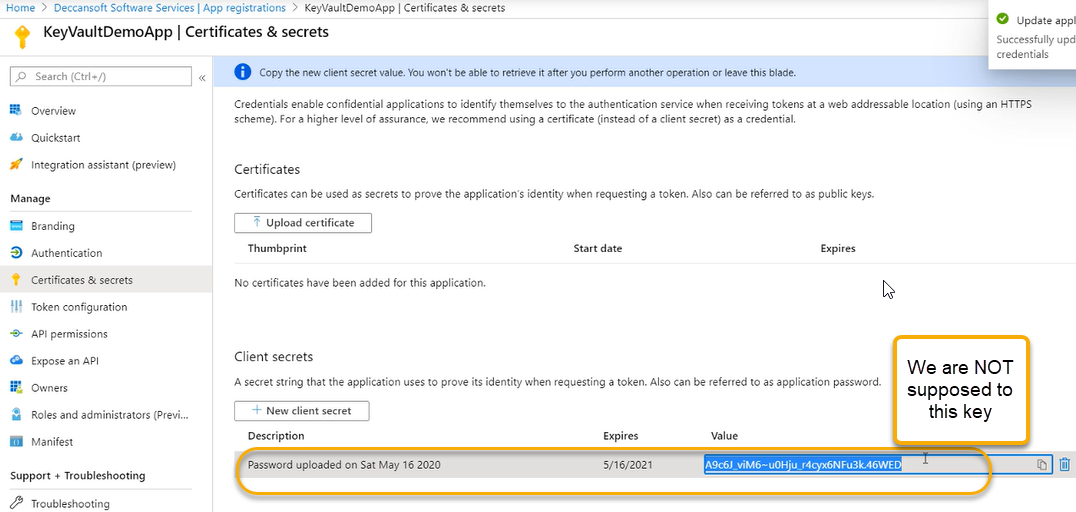


Anybody can execute the application those who has identity access and How programmer will take the identity of the application

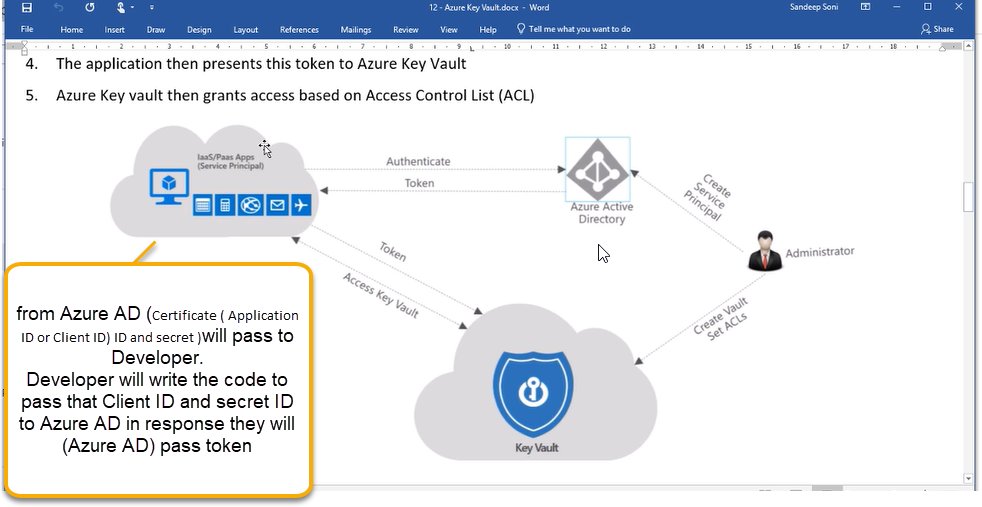
An active directory application has a unique ID which is called Application ID or Client ID







Certificate (Application ID or Client ID) ID and secret from above is what I am going to share the with the developer

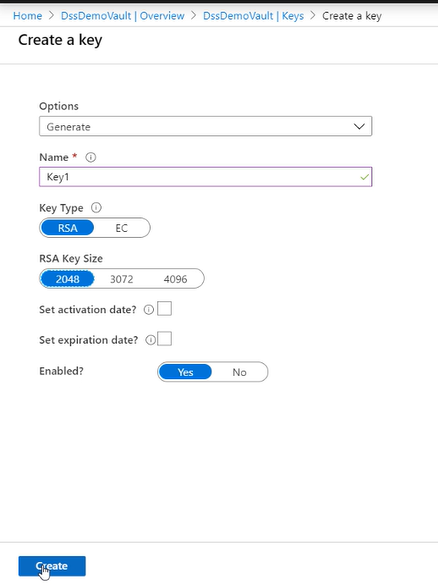


There are lot of services where we can go and properties configure the client id and secret for example if it is data engineer is working with data factory and if the data factory has to get data from key vault or data factory has to take data from some SQL database. Data factory can also use the same concept

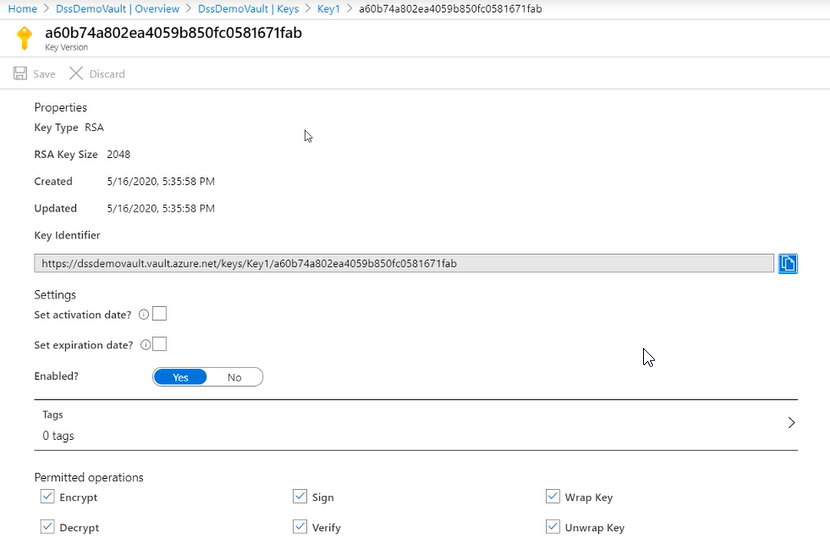
In the pipeline we will configure azure connection for accessing this Azure AD and this pipeline can use this identity to access the key vault.

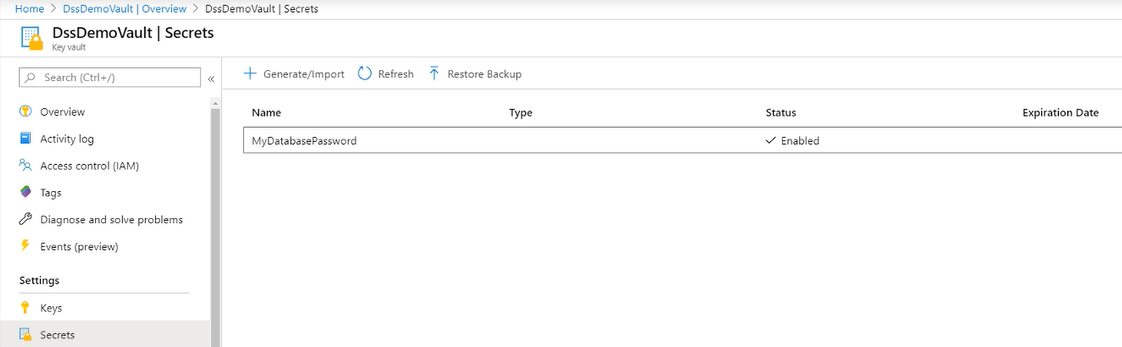
Many times in the pipeline we need some key values pair and even the pipeline owners are should not able to read this key

For the pipeline we will give service identity that means at the time of creating the pipeline we will have a service connection which is established with Azure Active Directory

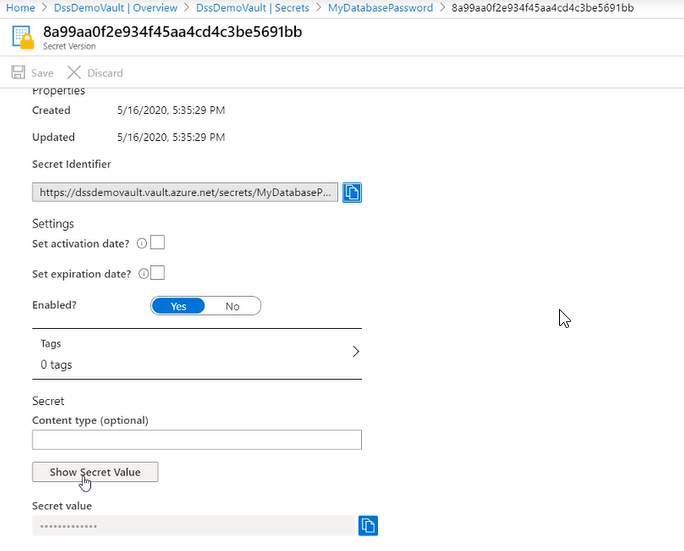


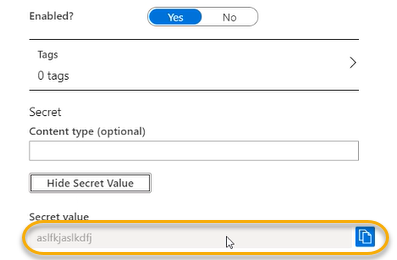


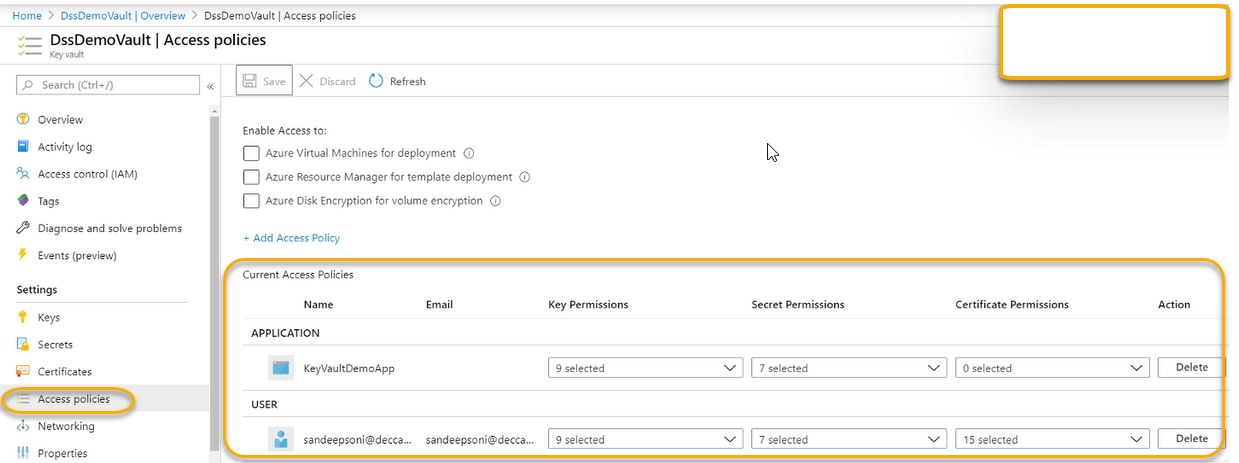


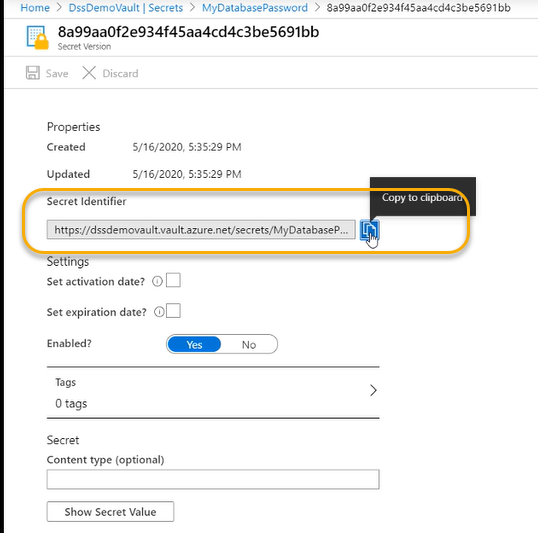


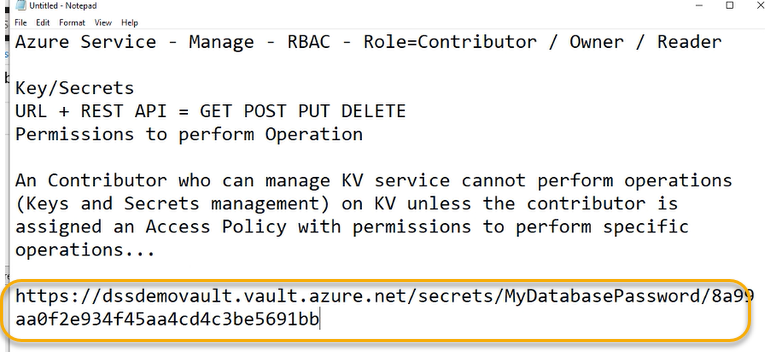




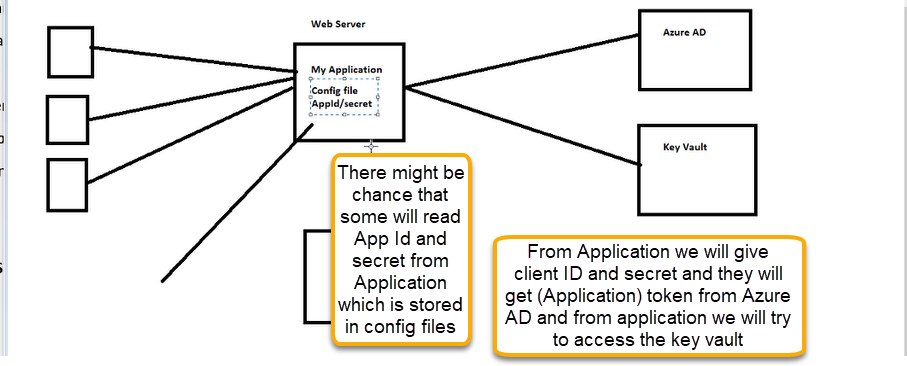






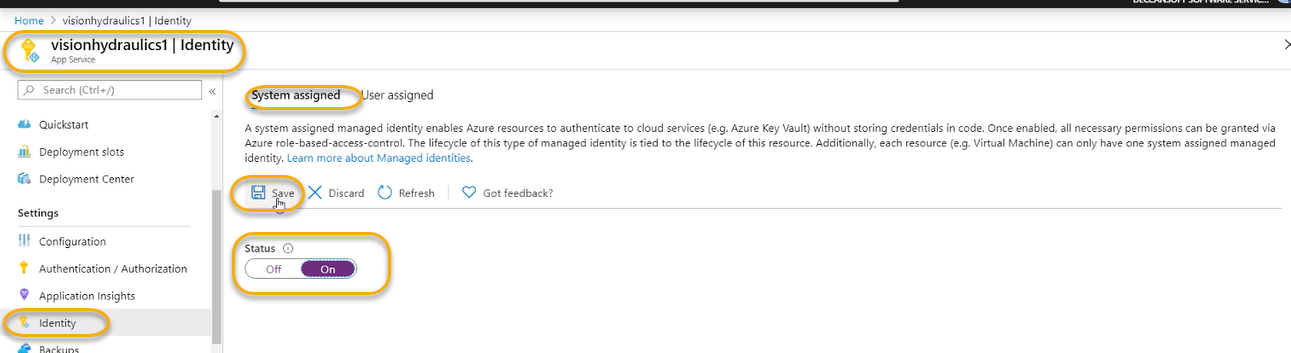


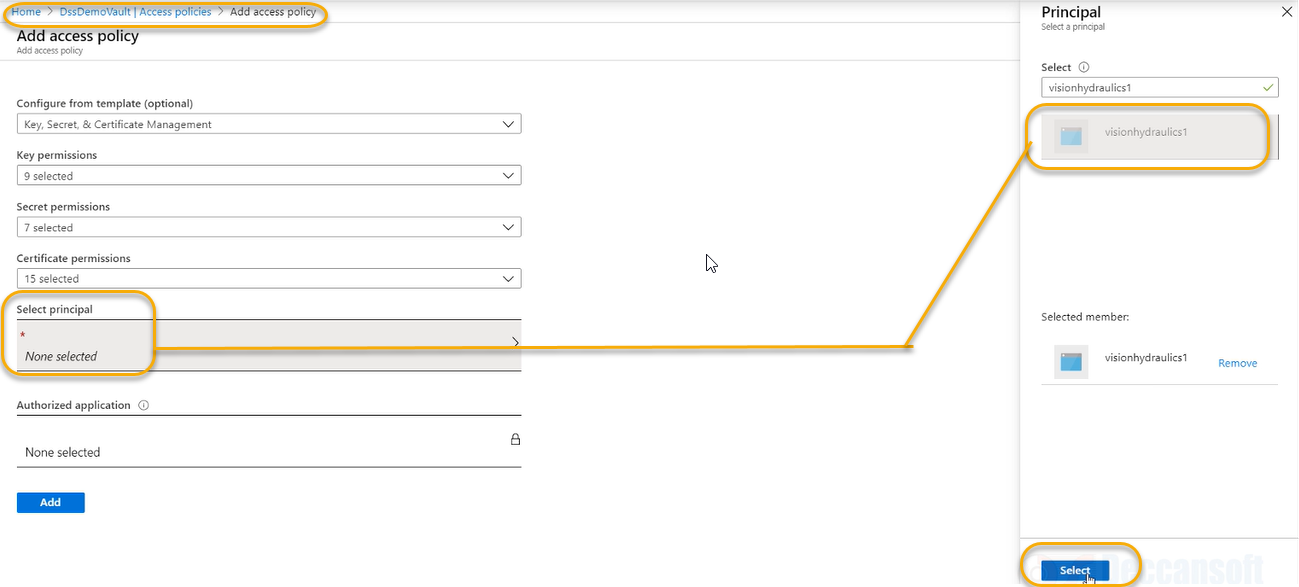
The above URL we need to give to developer and developer will take for reading the data in key vault



Whenever we create a VM/AppService obviously it is running inside the Azure ( Azure infrastructure)

For app service identity we are giving the system assigned identity





Add click on Add

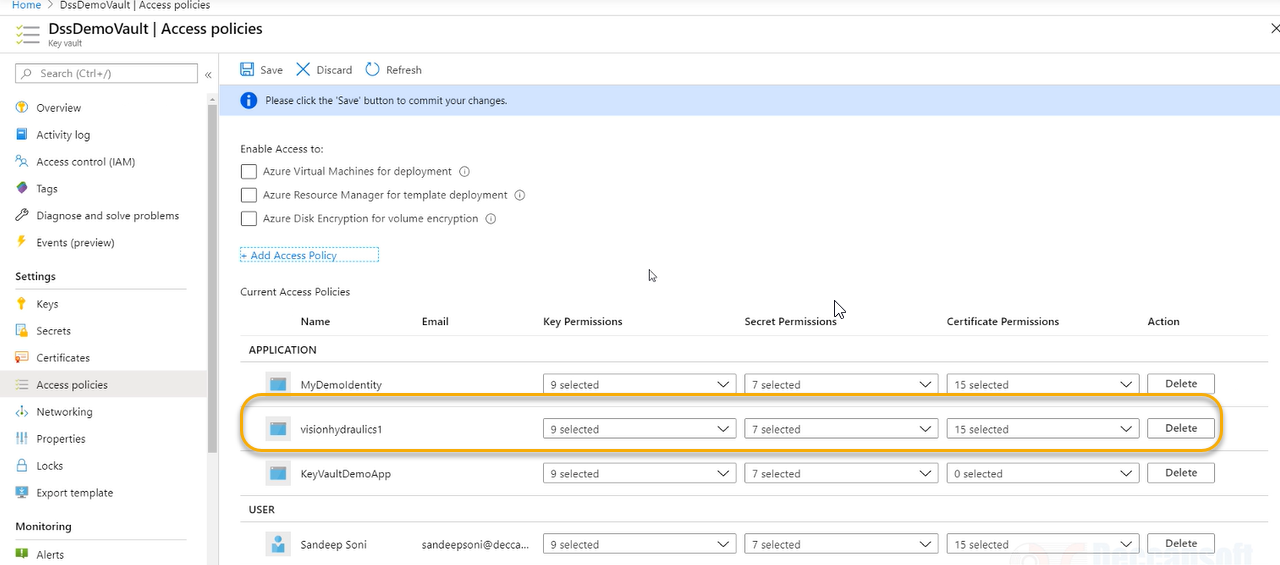


For every identity (VM or app service I need to go and add if it is 100 then we need to add 100 times

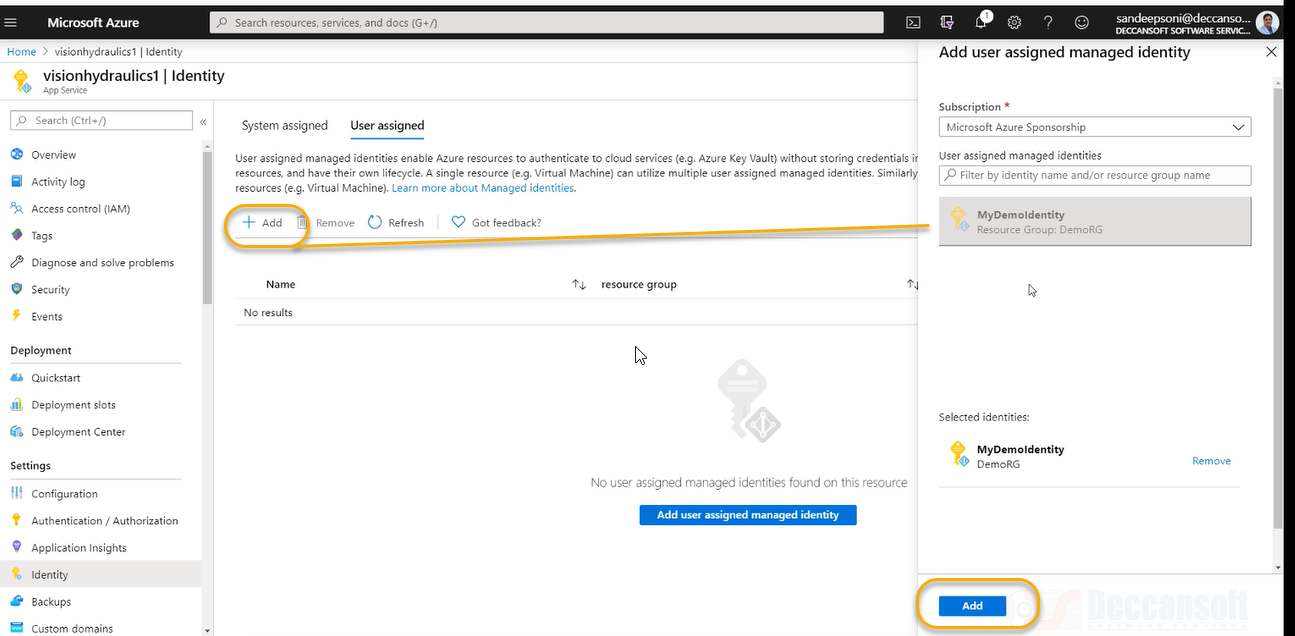
So, create the managed identity > Add



And in the key vault > Access policy > add permission for managed services



Now go to every appservices or VM



For every machine assign user assigned machine

