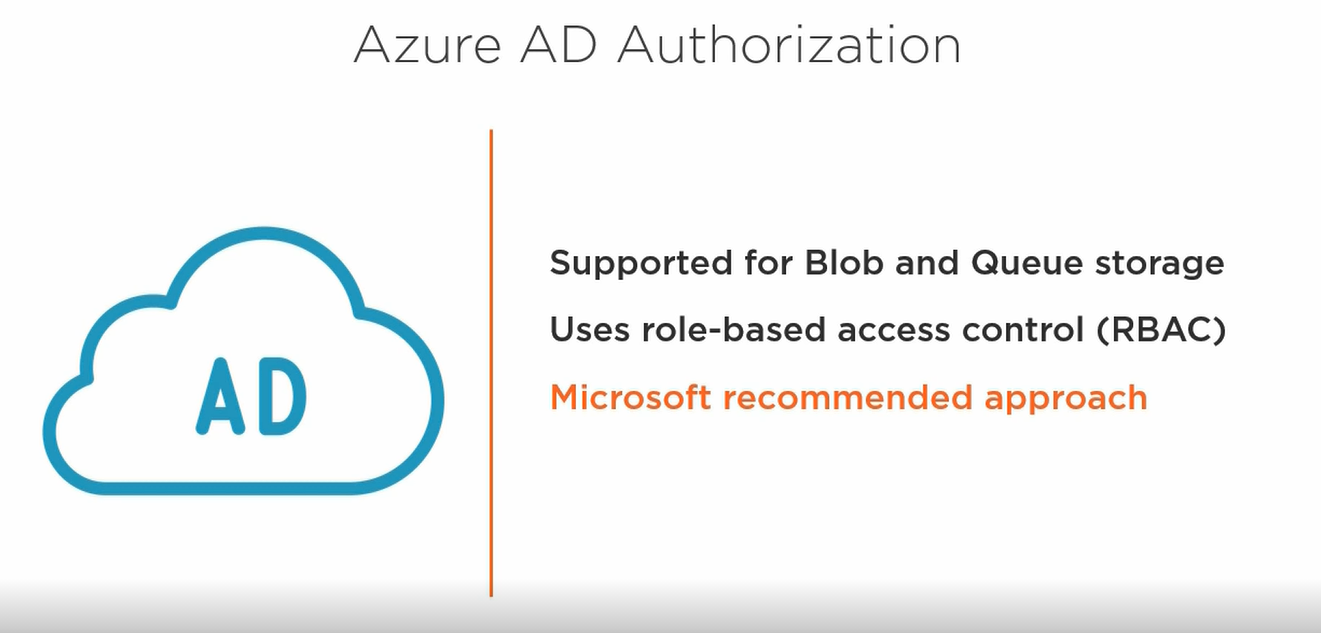
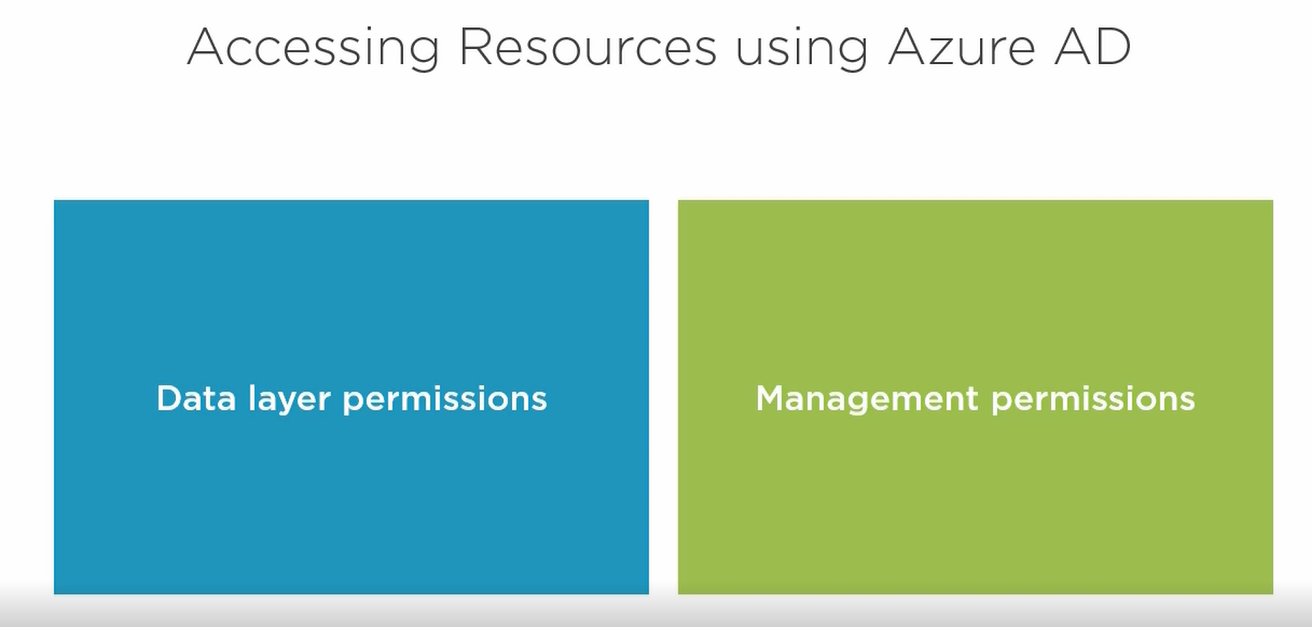
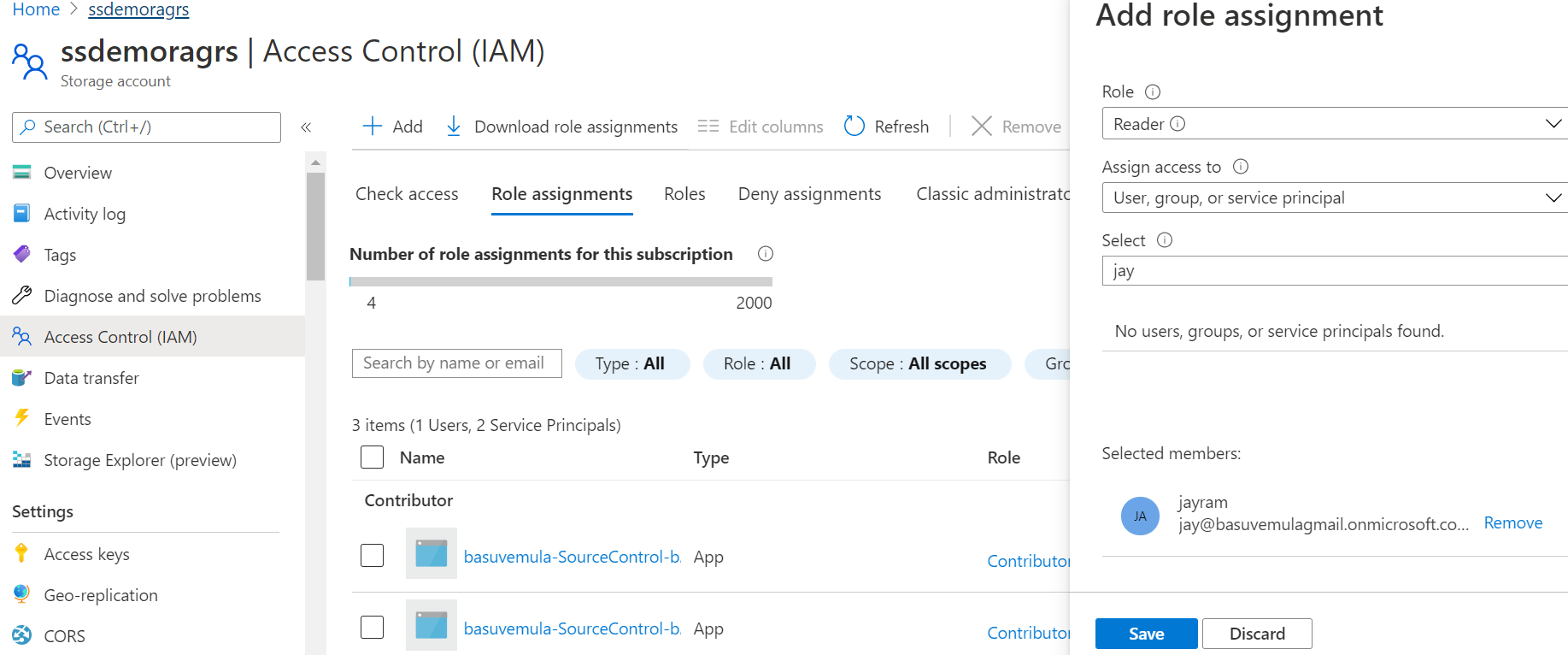
Azure Storage supports using Azure AD to authorize requests to Blob and Queue Storage. With Azure AD, you can use role‑based access control to grant permissions to a security principle, which may be a user, group, or application service principle. Authorizing access to Azure Storage with Azure AD provides a more secure and easier‑to‑implement method than using shared key authorization. Because of the security issues involved with shared keys, Microsoft recommends using Azure AD whenever possible



Before a service principle can access Azure Storage resources, it needs to have the proper permission sets. In this case, you need two sets of permissions. You need the **data layer permissions** for Azure Storage that allow you to access Blob and Queue data. There are a number of built‑in roles for this that you can assign. While this gives you storage access, it doesn't give you access to navigate through the resources in Azure. For that, you need access granted through **management permissions.** These permissions are assigned with an Azure resource manager role. The reader role is a good choice and gives the most restrictive permissions while providing the storage account access desired. Assignment of this role needs to be scoped at the storage account or higher, like a resource group or subscription, of course, depending on the breadth of access that the user needs, always looking at the principle of least privilege whenever applying any sort of permissions.

**In this demo, we want to give a user access to objects within our blob storage, or our SA “ssdemoragrs” storage account, and we want to use Azure AD authentication in order to do that.**

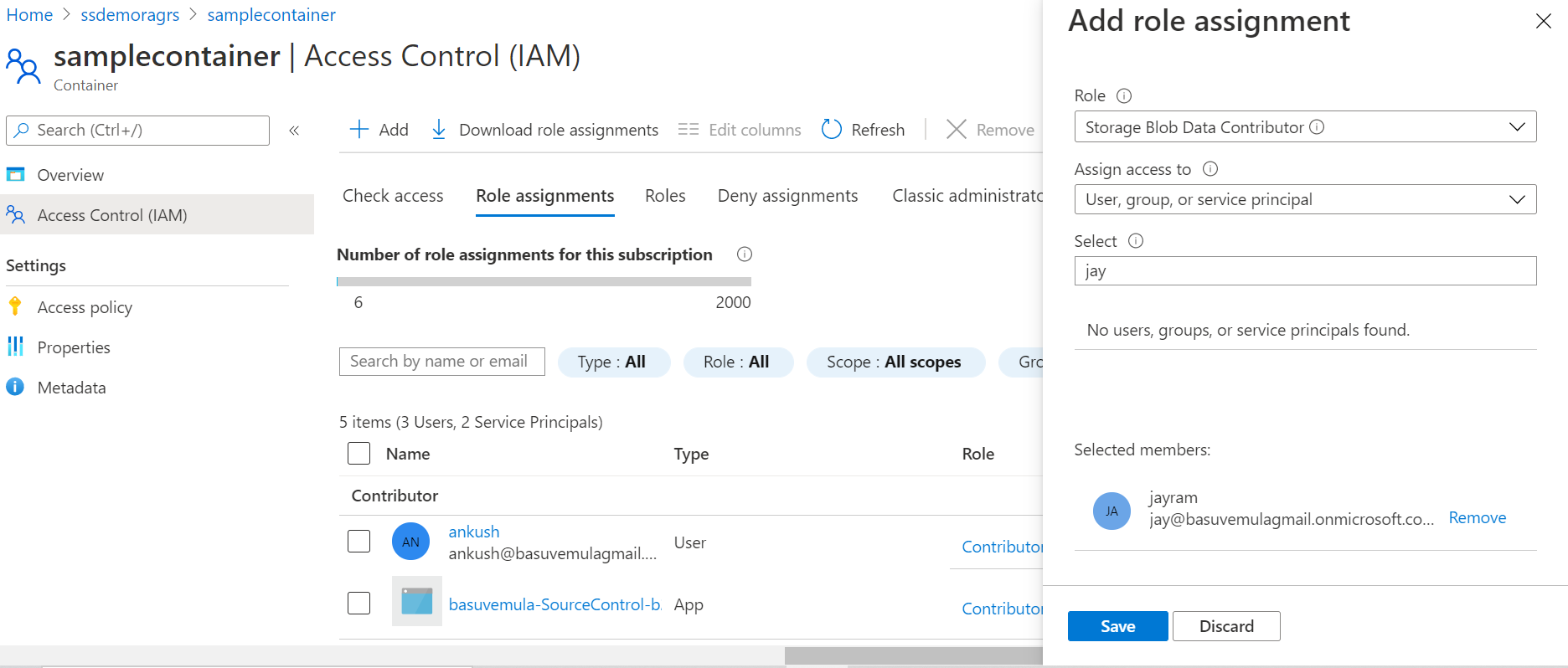
We have to set the data layer permissions and the management resource permissions. Set the management resource permissions first. Remember, we have to put that at the storage account or higher level, so I'm going to apply that to the storage account. So within the storage account blade, choose Access Control IAM, go to the role assignments, and we notice we have a few role assignments here. I'm going to go click add, add a role assignment. I'm going to choose the reader role because that's going to give the least amount of privilege for users to be able to get access to the documents within the objects within the storage account. And go ahead and look up the user name, choose his account, click save, and now the user has been saved.



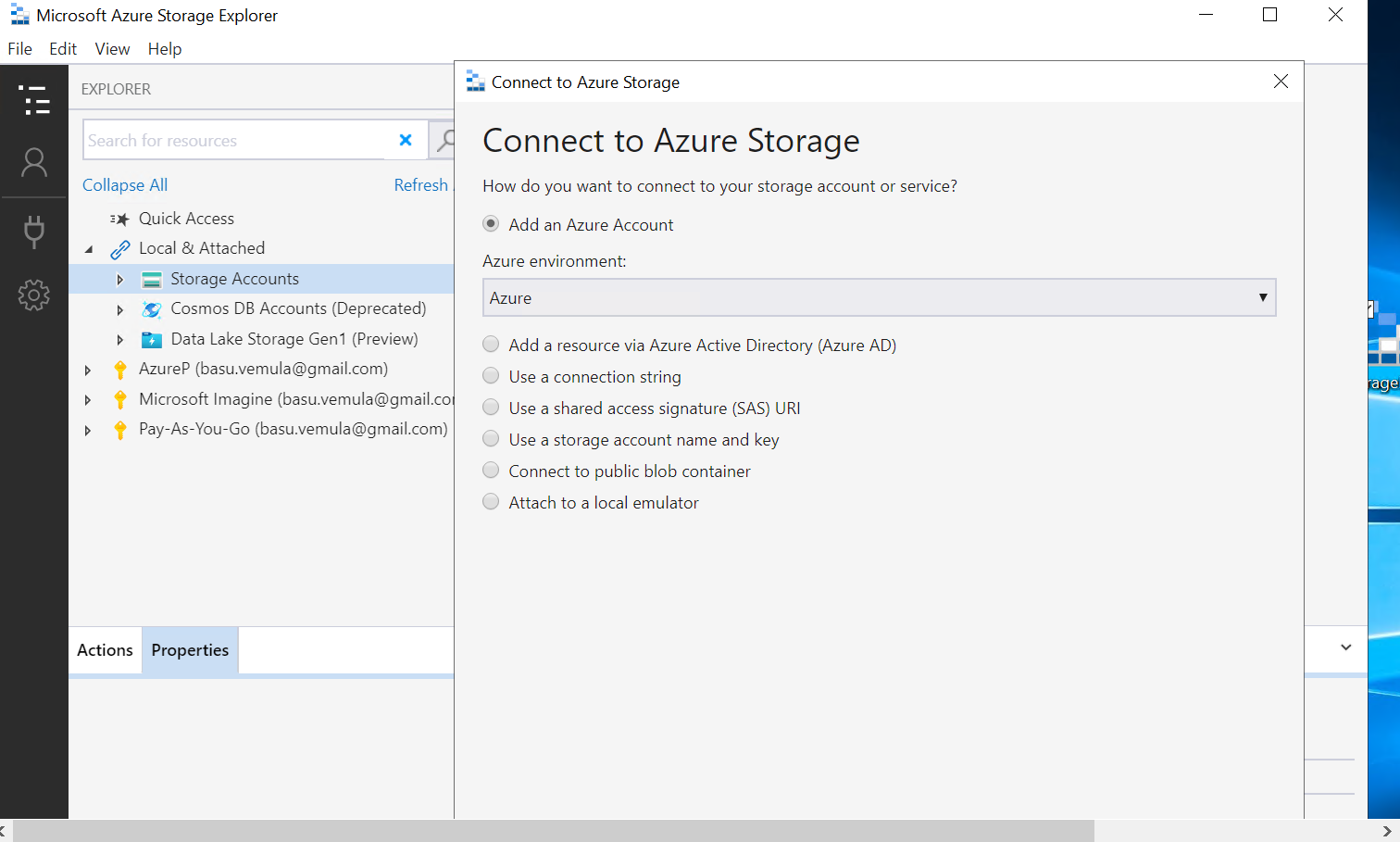
Now, go back up to overview, go into containers, go into samplecontainer, choose access control, and we're going to add a role assignment here. So if I type in blob, it gives me all of the blob roles. So we have a data contributor, owner, reader and delegator.

* Owner is going to allow you to change everything, including the permissions;
* the contributor is basically going to allow you to be able to add things and work with things within the storage container;
* the reader is basically going to allow you to be able to see what's inside of it.

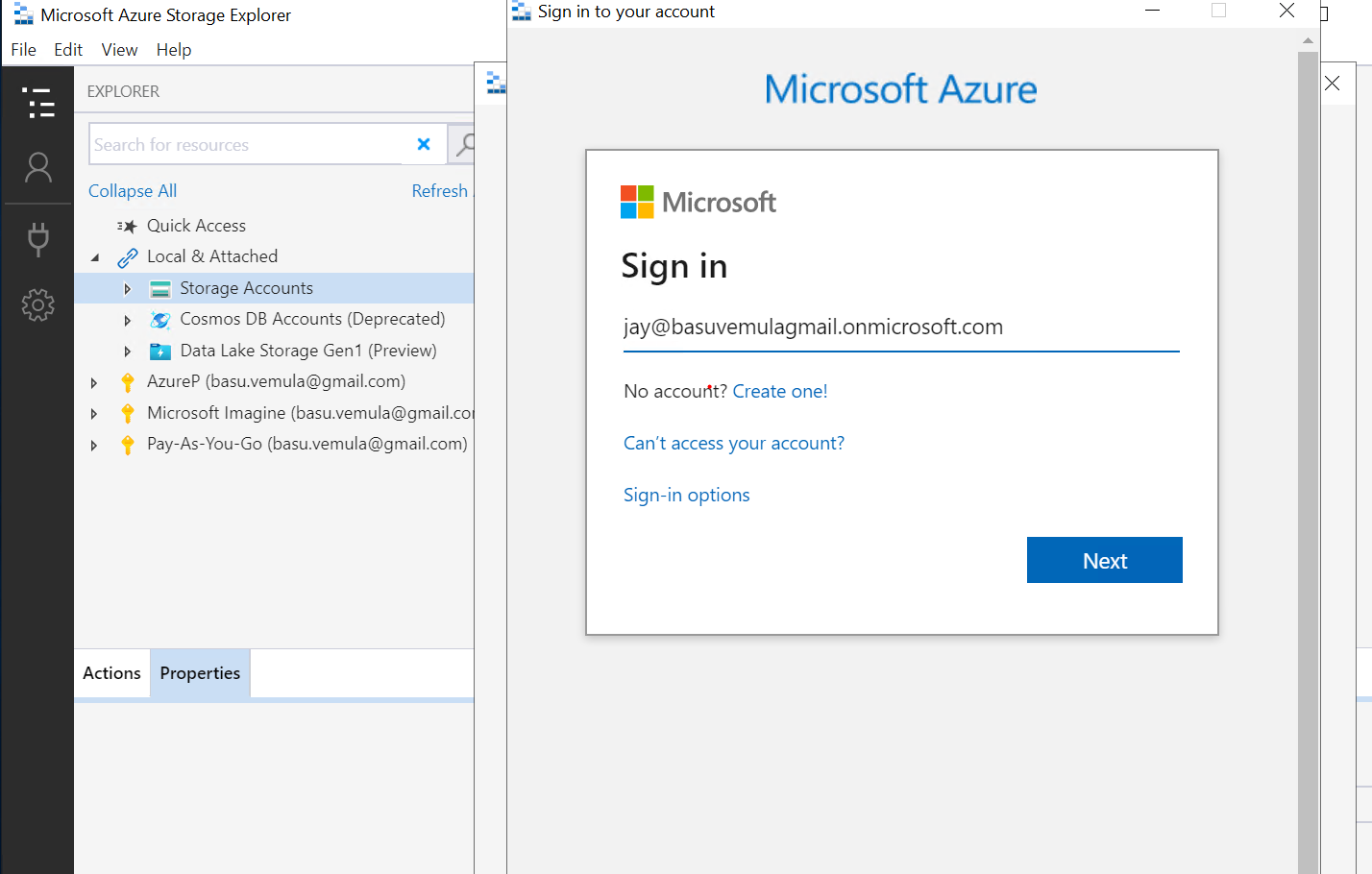
Choose a storage contributor, again search for the user's name, add user into there, and now user has been added with permissions for the samplecontainer



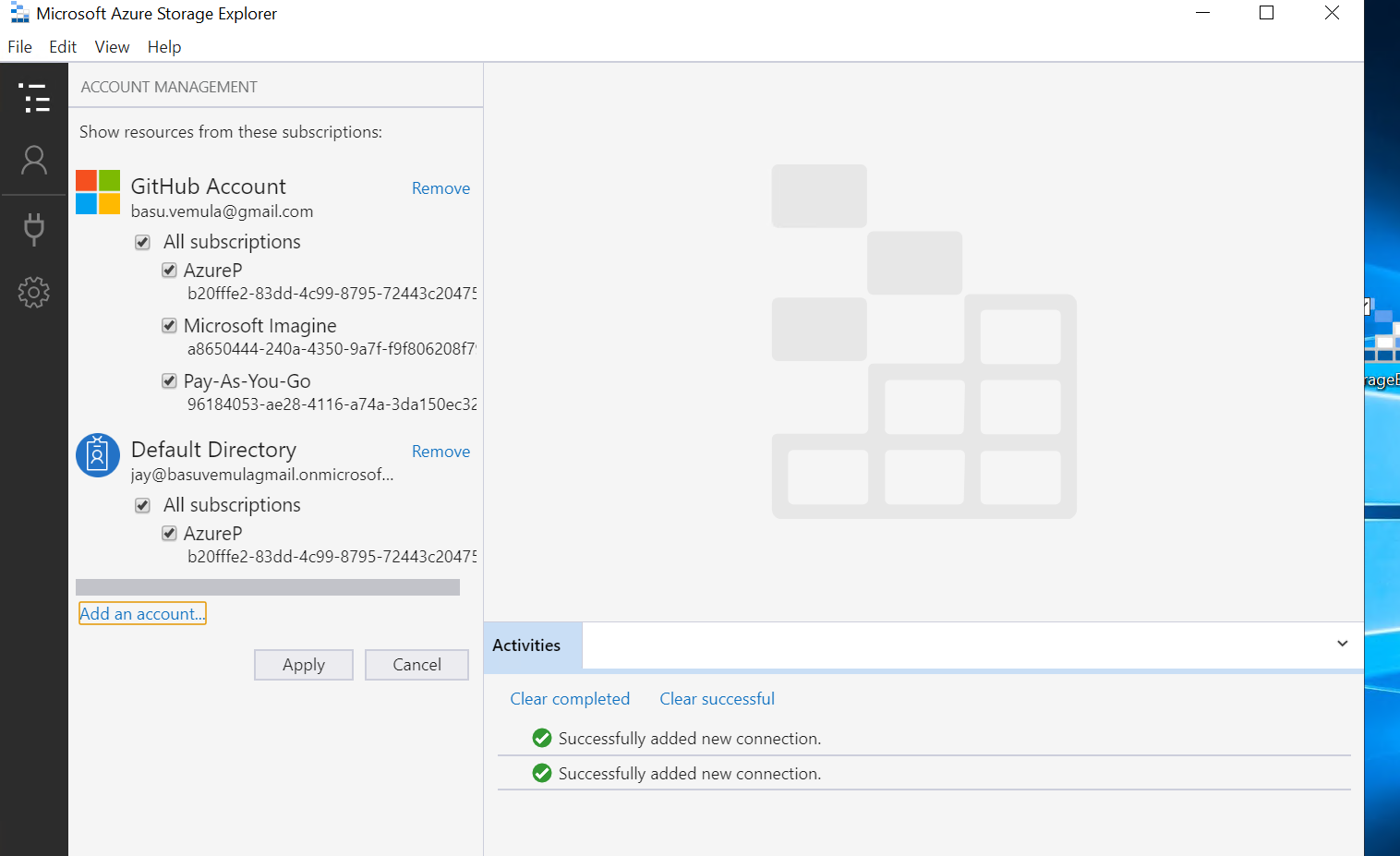
Now, go back over to our virtual machine, and connect with a storage explorer using Azure AD. So we click on the user icon, click add account, and choose add an Azure account.



Choose Azure, and then it's going to bring in the sign up box.

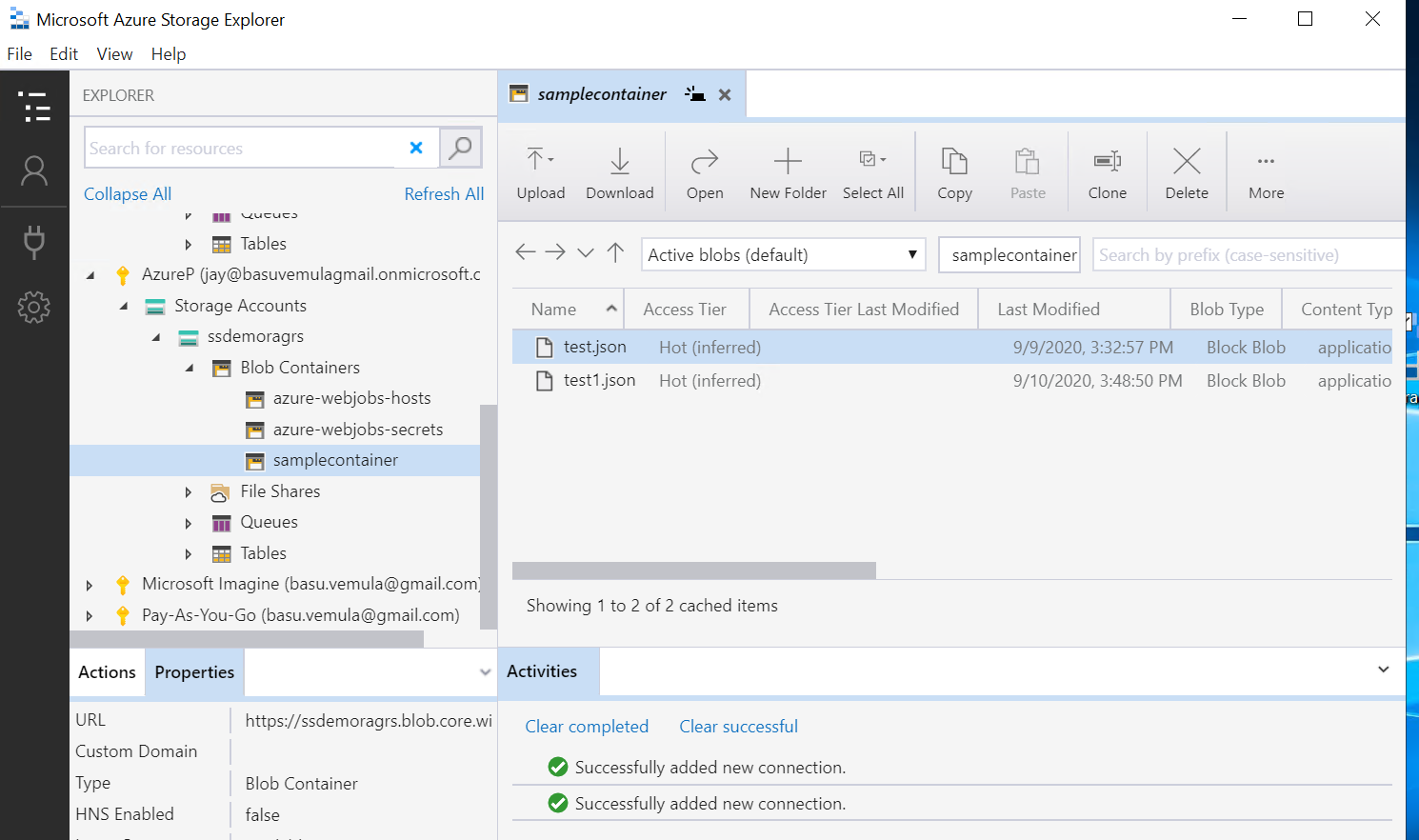


Put in user credentials, wait for authentication, and notice it brings up the subscription that user has access to, I'll go ahead and click apply. Now we see that it added that subscription into the storage account.



then connect the Azure storage into my storage account. At this point, choose a resource via Azure Active Directory because I have my account added in, which we choose as a user account, we put in the container URL, it's going to be **https://ssdemoragrs.blob.core.windows.net/samplecontainer**

Click next, click connect, and now we see that that's connected in. So we have access to the documents here. If I wanted to upload, I could work with those. If I wanted to remove that text file, that allows us to remove it



If I try to access other files or queues, notice that it gives me an authorization warning because I don't have access, remember I set the Azure Active Directory to that specific container and not to all of the services or containers

