Acquiring Azure AD credentials for blob storage

Microsoft recommends transitioning away from Shared Key authorization for Azure Storage in favor of using Azure AD. This cheat sheet describes how to create credentials in Azure AD for use with WCSM.

The process is a two-stage process. In the first stage create a service principal and register it with the AD. Please note this service principal represents/acts on behalf of the WCSM platform. In the second stage allow service principal through a role assignment process, to access the storage account.

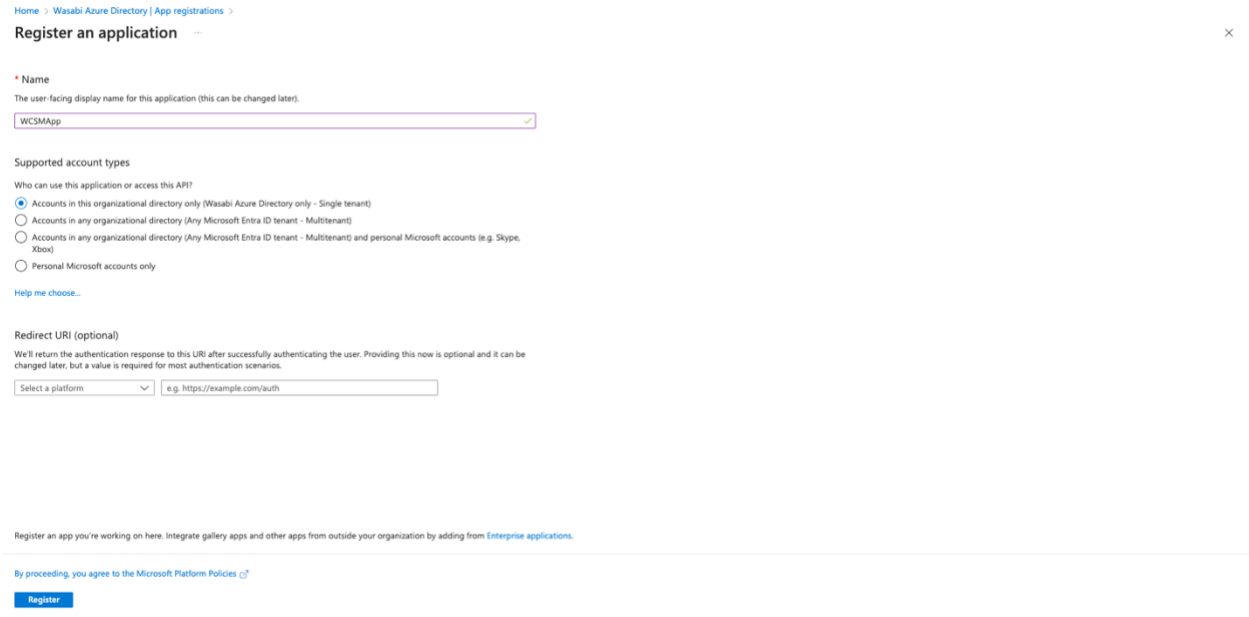
Service Principal Creation and App registration

Step 1: Search for “Microsoft Entra ID” and click on it.

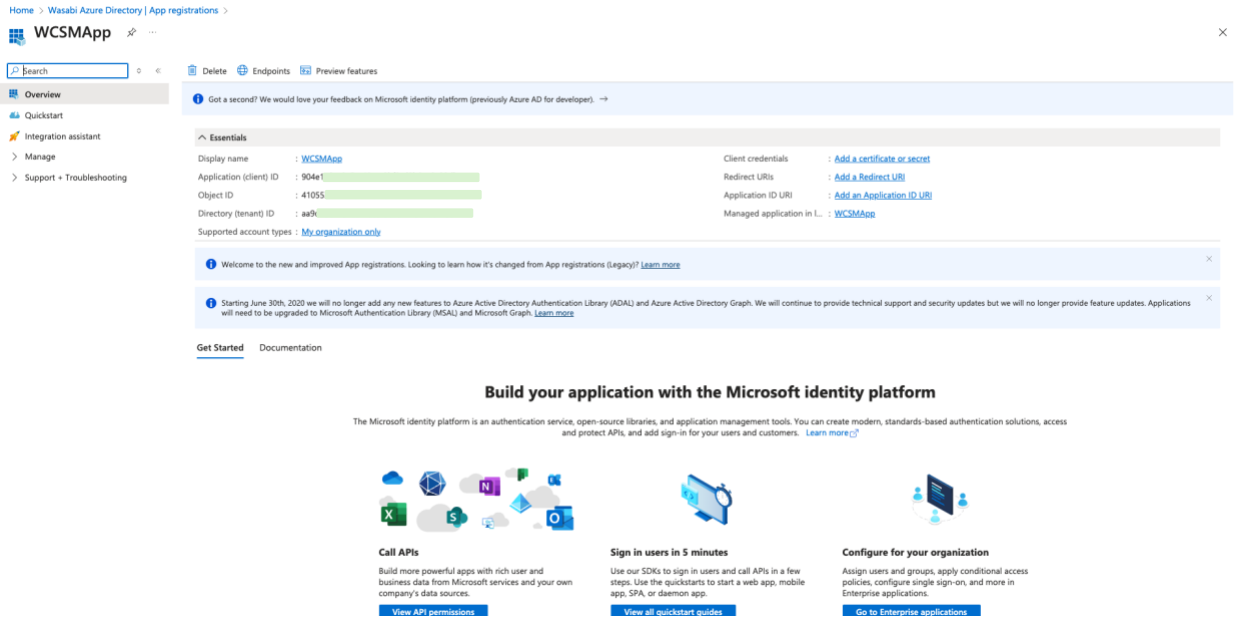
Step 2: Under “Manage” on the side menu click on “App registrations”

Step 3: Click on “+ New registration” in the top menu

Step 4: Enter a name, e.g. “WCSMApp” (or any other name of your choosing). And choose “Accounts in this organizational directory only (xxx Azure Directory only – single tenant)”. And then press “Register”



Step 5: You will see details about the newly registered app here, including, “Application (client) ID”, Directory (tenant) ID here. **Note down the “Application (client) ID” and Directory (tenant) ID”** (you can come back to it later as well).



Step 6: Click on “Client Credentials: “Add a certificate or secret”

Step 7: Click on “+ New client secret”. Enter description and press “Add”.

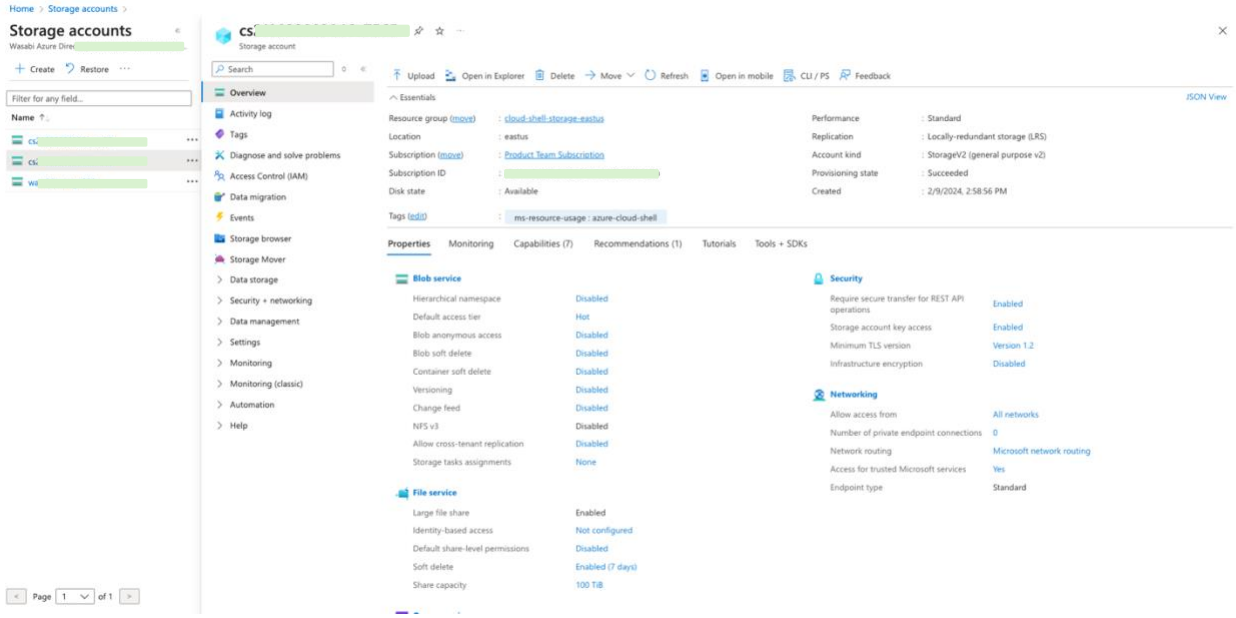
Step 8: Note down the “Value” and “secret ID” values. (The value is only visible once). If you miss noting it down, you can come back to create new client secret.

At this point you have all the information that is required for WCSM. Use the “Tenant ID” and “Client ID” from Step 5 AND “Secret ID” and “Value” from Step 7 to specify the source bucket “Credentials” in WCSM.

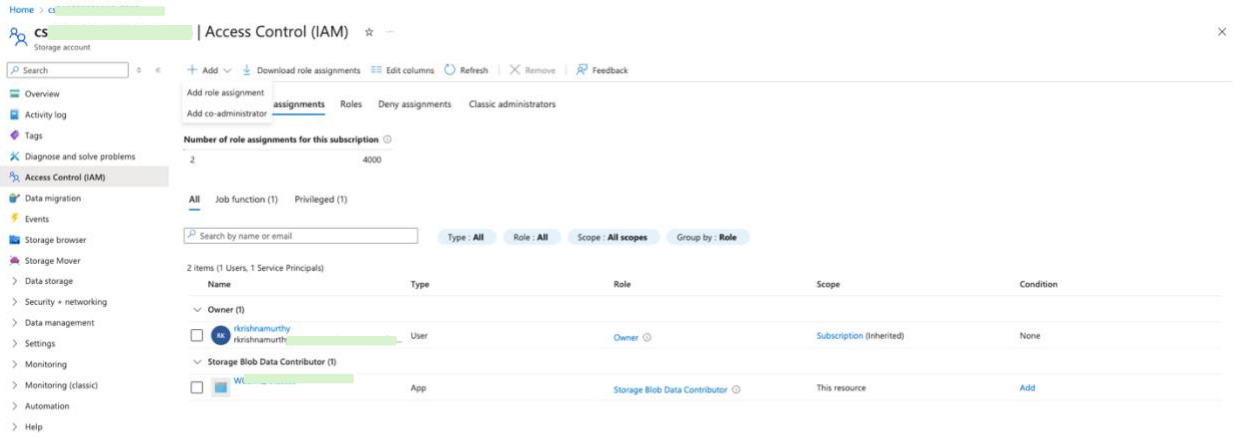
Storage account role assignment to the Service Principal

This step is required to allow the Service Principal created to access the storage account containing the blob storage.

Step 1: Go to your “Storage accounts” and click on the storage account containing source data.



Step 2: Click on “Access Control (IAM)” tab on the left and click on “Role assignments” and then press “Add” and choose “Add role assignment”



Step 3: Search for and select “Storage Blob Data Reader”. Search for and select “Storage Blob Data Contributor”. And press next.

Step 4: Press “+Select member” and search for and select “WCSMApp” (or the name you had used for “App registration” process in Step 4). And press “Next”