## 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"

* Name	
The user-facing display name for this	application (this can be changed later).
WCSMApp	×.
Supported account types	
Who can use this application or accer	s this API?
<ul> <li>Accounts in this organizational d</li> </ul>	irectory only (Wasabi Azure Directory only - Single tenant)
O Accounts in any organizational d	irectory (Any Microsoft Entra ID tenant - Multitenant)
<ul> <li>Accounts in any organizational d Xbox)</li> </ul>	irectory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype,
O Personal Microsoft accounts only	
Help me choose	
Redirect URI (optional)	
We'll return the authentication respon changed later, but a value is required	use to this URI after successfully authenticating the user. Providing this now is optional and it can be for most authentication scenarios.
Select a platform	e.g. https://example.com/auth
Bendeter an environmental second to a second	so interests college ages and other ages from outside your experiention by adding from Enterprise and enter

**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).

Home > Wasabi Azure Directory   App re	gistrations >				×			
ρ βearch o «	📋 Delete 🌐 Endpoints 🔤 Preview	features						
R Overview	Got a second? We would love your feed	back on Microsoft identity platform (previously Azure AD for de	veloper). $\rightarrow$					
di Quickstart								
🛒 Integration assistant								
> Manage	Display name : WCSMApp		Client credentials	: Add.a.certificate.or.secret				
> Support + Troubleshooting	Application (client) ID : 904e1		Redirect URIs	: Add a Redirect URI				
	Object ID : 41055		Application ID URI	: Add an Application ID URI				
	Directory (tenant) ID : aa9		Managed application in	L. : WCSMApp				
	Supported account types : My organiza	tion only						
	Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more							
	Starting June 30h, 2020 we will no longer add any new features to Asure Active Directory Authentication Library (ADAL) and Asure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Library nova							
	Get Started Documentation							
		Build your	application with the Microsoft id	dentity platform				
		The Microsoft identity platform is an authentication servi	ce, open-source libraries, and application management tools. You and protect APIs, and add sign-in for your users and customers. La	can create modern, standards-based authentication solutions, access ann more උ				
				e 💽 🕴				
		Call APIs	Sign in users in 5 minutes	Configure for your organization				
		Build more powerful apps with rich user and business data from Microsoft services and your or company's data sources.	Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.	Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.				
		View API permissions	View all quickstart guides	Go to Enterprise applications				

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.

Storage accounts	os cs	\$ \$ T						×
wasaoi Azure Dire	storage account							
+ Create > Restore	D search	🕈 Upload 🚡 Open in Explorer 🗐 🛙	Delete $\rightarrow$ Move $\checkmark$ 🕐 Refresh	Open in mobile	CLI / PS 🔗 Feedback			
Filter for any field	Overview							JSON View
Name 🕆	Activity log	Resource group (move) : cloud-shell-s	torage eastus		Performance	: Standard		
= 0	Tags	Location : eastus			Replication	: Locally-redund	ant storage (LRS)	
= ~ …	X Diagnose and solve problems	Subscription (move) : Product Team	n Subscription		Account kind	1 StorageV2 (gen	eral purpose v2)	
-	Access Control (IAM)	Subscription ID :		Provisioning state	: Succeeded	: Succeeded		
- **	Pata migration	Disk state : Available			Created	: 2/9/2024, 2:58:	56 PM	
	5 Events	Tags (edit) : ms-resour	rce-usage : azure-cloud-shell					
	Storage browser		-					
	Storage Mover	Properties Monitoring Capabilitie	es (7) Recommendations (1)	Tutonais Tools + SD	KS			
	Data storage	Eleb service			O. Security			
	> Data storage	Miararchical namarnara	Dirabled		Require cercum tran	der for REST AD		
	> security + networking	Default access tier	blog		operations		Enabled	
	> Data management	Biob accountancess	Disabled		Storage account key	/ access	Enabled	
	> Settings	Blob soft delete	Dirabled		Minimum TLS version	an l	Version 1.2	
	> Monitoring	Container soft delete	Disabled		Infrastructure encry	ption	Disabled	
	> Monitoring (classic)	Versioning	Disabled					
	> Automation	Change feed	Disabled		Se Networking			
	> Help	NFS v3	Disabled		Allow access from		All networks	
		Allow cross-tenant replication	Disabled		Number of private e	endpoint connections	0	
		Storage tasks assignments	None		Network routing		Microsoft network routing	
					Access for trusted N	Acrosoft services	Yes	
		File service			Endpoint type		Standard	
		Large file share	Enabled					
		Identity-based access	Not configured					
		Default share-level permissions	Disabled					
		Soft delete	Enabled (7 days)					
Page 1 x of 1		Share capacity	100 T/B					
i alla		117 <u>117</u> 11						

**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"

Home > cs								
R CS Storage account	Access Control (IAM) *							
₽ Search 0 €	$+$ Add $\lor$ $\frac{1}{2}$ Download role assignments $\equiv$ Ed	it columns 🜔 Refresh 🛛 🗙 Remove 🗍 👰 Fi	eedback					
Overview     Activity log	Add role suignment Add co-administrator Roles Deny assignments Classic administrators							
Tags	Number of role assignments for this subscription 🕓							
× Diagnose and solve problems	2 4000							
Recess Control (IAM)								
<ul> <li>Data migration</li> <li>Events</li> </ul>	All Job function (1) Privileged (1)							
Torage browser	P Search by name or email	Type : All Role : All Scope	e : All scopes Group by : Role					
<ul> <li>Storage Mover</li> <li>Data storage</li> </ul>	2 items (1 Users, 1 Service Principals) Name	Туре	Role	Scope	Condition			
> Security + networking	A Description							
> Data management	<ul> <li>owner (i)</li> <li>drishnamurthy</li> </ul>							
> Settings	rkrishnamurth	User	Owner 💿	Subscription (Inherited)	None			
> Monitoring								
> Monitoring (classic)	C = W	App	Storage Blob Data Contributor ()	This resource	Add			
> Automation								
> Help								

**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"