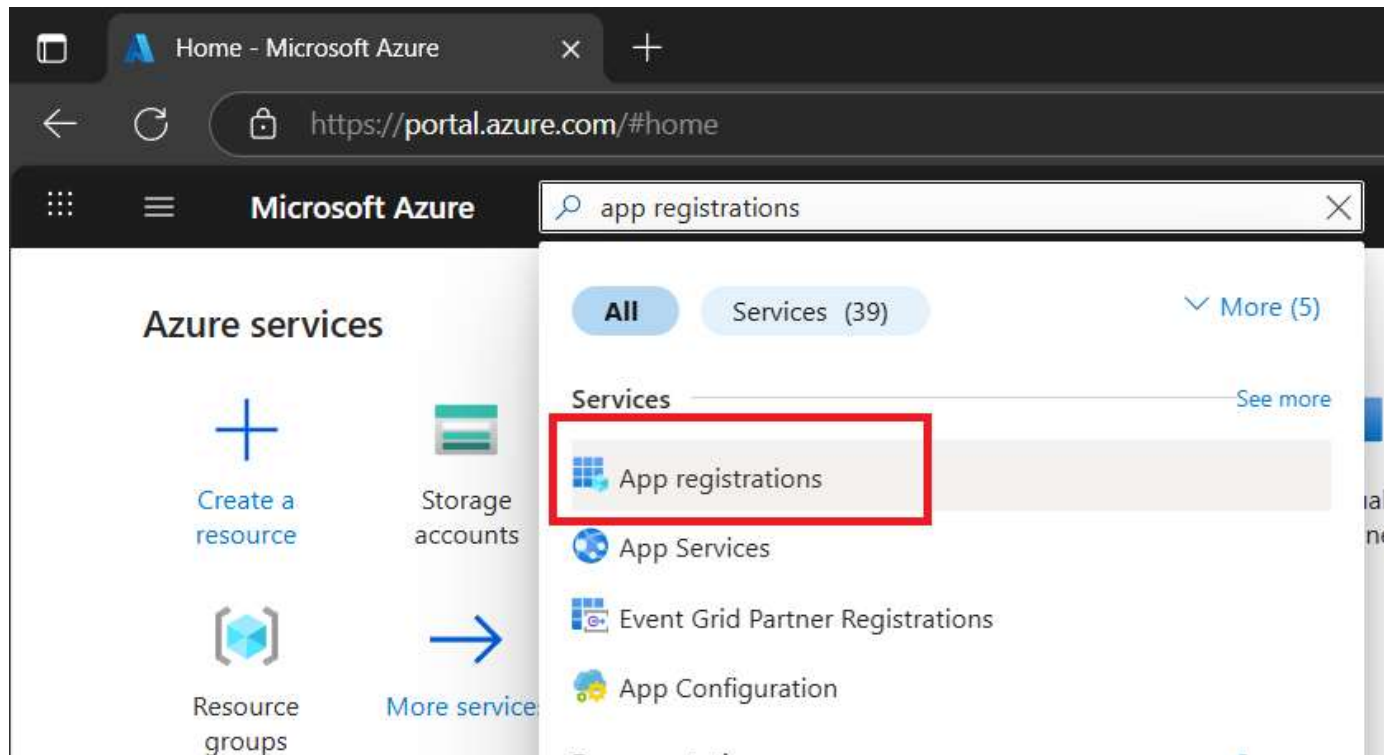


## Creating an App Registration (SPN/AppID) for AVD Environments

Here's a step by step approach to creating an App Registration (also known as Service Principal Name (SPN) or App ID) which will be used to authenticate with your AVD infrastructure in Azure to manage locked profiles on Azure File Shares and/or retrieve hosts and session information from AVD host pools so that users can logout and end their own hung sessions.

### Step 1 - Create an App Registration


In the Azure Portal, type "app registrations" and select it.




Click "New Registration", and in the next screen, give it a name and click "Register."

[Home](#) >

## App registrations

 [New registration](#)

 [Endpoints](#)

 [Troubleshoot](#)

 [Refresh](#)

 [Download](#)

 [Preview](#)

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication continue to provide technical support and security updates but we will no longer provide feature updates for Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)


[All applications](#)

[Owned applications](#)

[Deleted applications](#)

[Applications from person](#)

 Start typing a display name or application (client) ID to filter these r...

 [Add filters](#)

## Register an application ...

**\* Name**

The user-facing display name for this application (this can be changed later).

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and Xbox
- Personal Microsoft accounts only

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Write down the Application ID and Directory (tenant) ID. Then, click "Add a certificate or secret."

Home > App registrations >

# FixMySession

Search [x] [back] [Delete] [Endpoints] [Preview features]

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions

### Essentials


Display name <a href="#">FixMySession</a>	Client credentials <a href="#">Add a certificate or secret</a>
Application (client) ID dc	Redirect URIs <a href="#">Add a Redirect URI</a>
Object ID 24	Application ID URI <a href="#">Add an Application ID URI</a>
Directory (tenant) ID d0	Managed application in local directory <a href="#">FixMySession</a>
Supported account types <a href="#">My organization only</a>	










Click "New Client Secret," then type in a Client Secret Name and choose your preferred Secret Expiration period. When this secret expiration period elapses, you will need to create a new client secret in order for Fix My Session to continue working.

Home > App registrations > FixMySession

## FixMySession | Certificates & secrets



 Got feedback?

-  Overview
-  Quickstart
-  Integration assistant
-  Diagnose and solve problems
- ▼ Manage
  -  Branding & properties
  -  Authentication
  -  **Certificates & secrets**
  -  Token configuration
  -  API permissions

Credentials enable confidential applications to identify themselves to the a web addressable location (using an HTTPS scheme). For a higher level (instead of a client secret) as a credential.

 Application registration certificates, secrets and federated credentials c

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requ application password.



# FixMySession | Certificates & secrets

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting
  - New support request

Credentials enable com...  
a web addressable loca...  
(instead of a client secr...

Application regist...

Certificates (0)

A secret string that th...  
application password.

+ New client secre...

Description

No client secrets have...

## Add a client secret

Description

Expires

**IMPORTANT: Now immediately copy the Client Secret Value to the clipboard and save it alongside the Application ID and Tenant ID above. You will need to supply this credential information to Fix My Session when configuring it.**

FixMySession | Certificates & secrets

Search

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

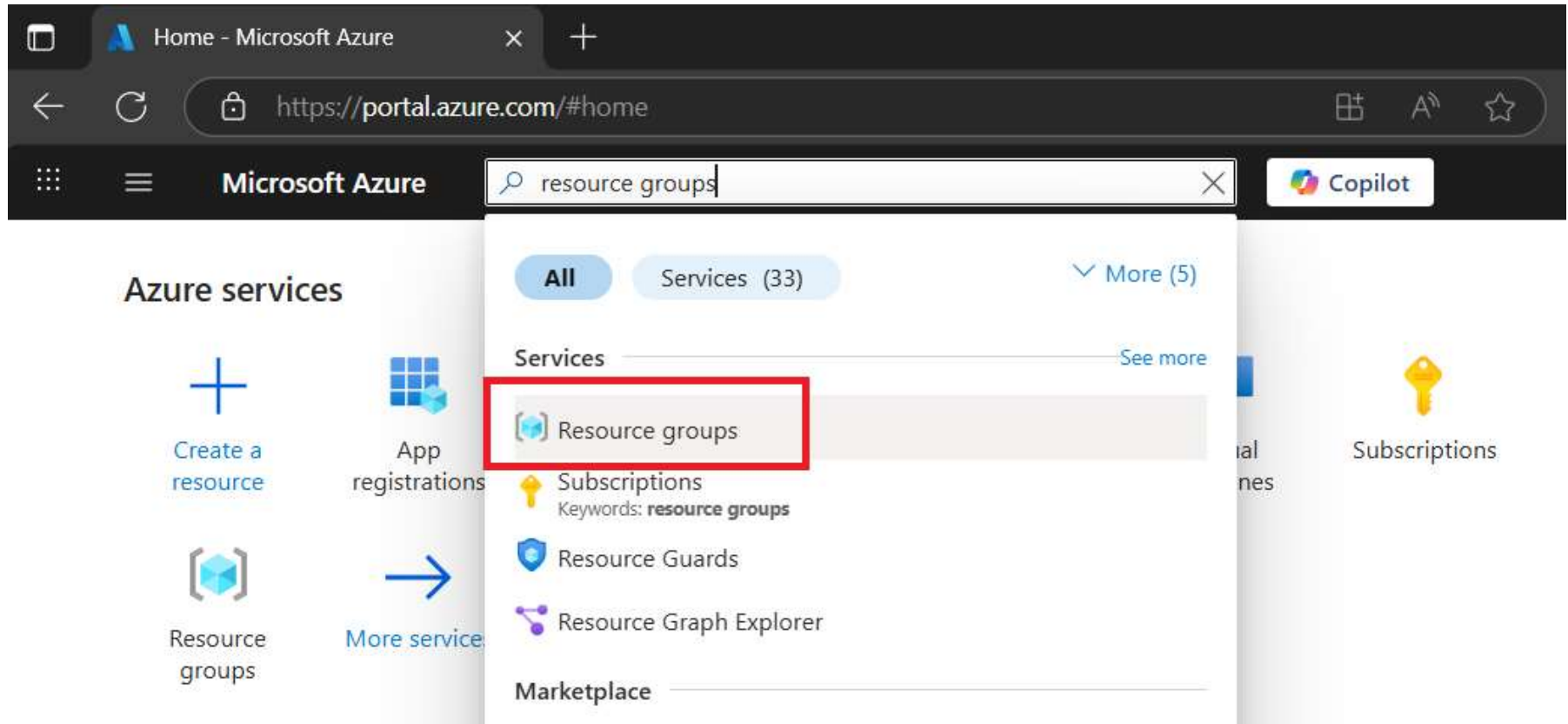
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Copy to clipboard	App ID
FixMySessionSecret	7/18/2027	randomsecretpwchars		

## Step 2 - Assign IAM Roles To Your App Registration

In the Azure Portal, type "resource groups" and select it.



Click on the name of the Resource Group that houses your AVD host pools.

# Resource groups ...

Default Directory

 Create  Manage view  Refresh  Export to CSV  Open

 [You are viewing a new version of Browse experience. Click here to access the old e](#)

 wvd 

Subscription equals **all**

Location equals

Name ↑

 WVD 

Make a note of the Subscription ID of this resource group. You will need this information later when supplying credentials to the Fix My Session application. Then, click "Access Control (IAM)."

WVD  
Resource group

Search

Overview

Activity log

**Access control (IAM)**

Tags

Resource visualizer

Events

Create Manage view Delete res

Essentials

Subscription ([move](#))

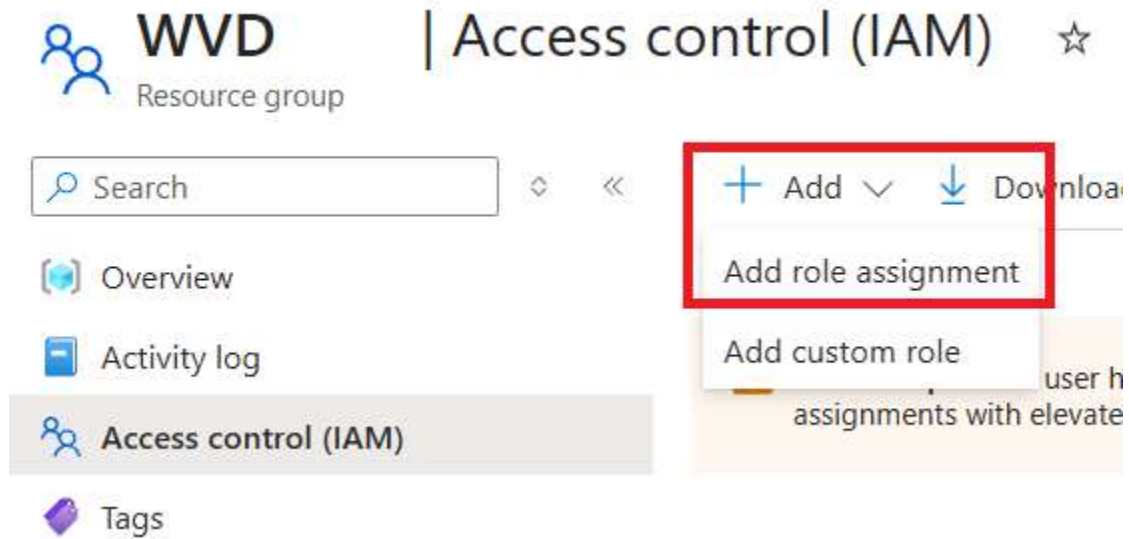
[Microsoft Azure Sponsorship](#)

Subscription ID		
50	19-9	fd5

Tags ([edit](#))

[Add tags](#)

Click on the "+Add" menu to add a role assignment.



Search for the **Desktop Virtualization Contributor** Role, select it, and click "Next."

## Add role assignment

[Role](#) [Members](#) [Conditions](#) [Review + assign](#)

A role definition is a collection of permissions. You can use the built-in roles or you can

[Job function roles](#) [Privileged administrator roles](#)

Grant access to Azure resources based on job function, such as the ability to create vir

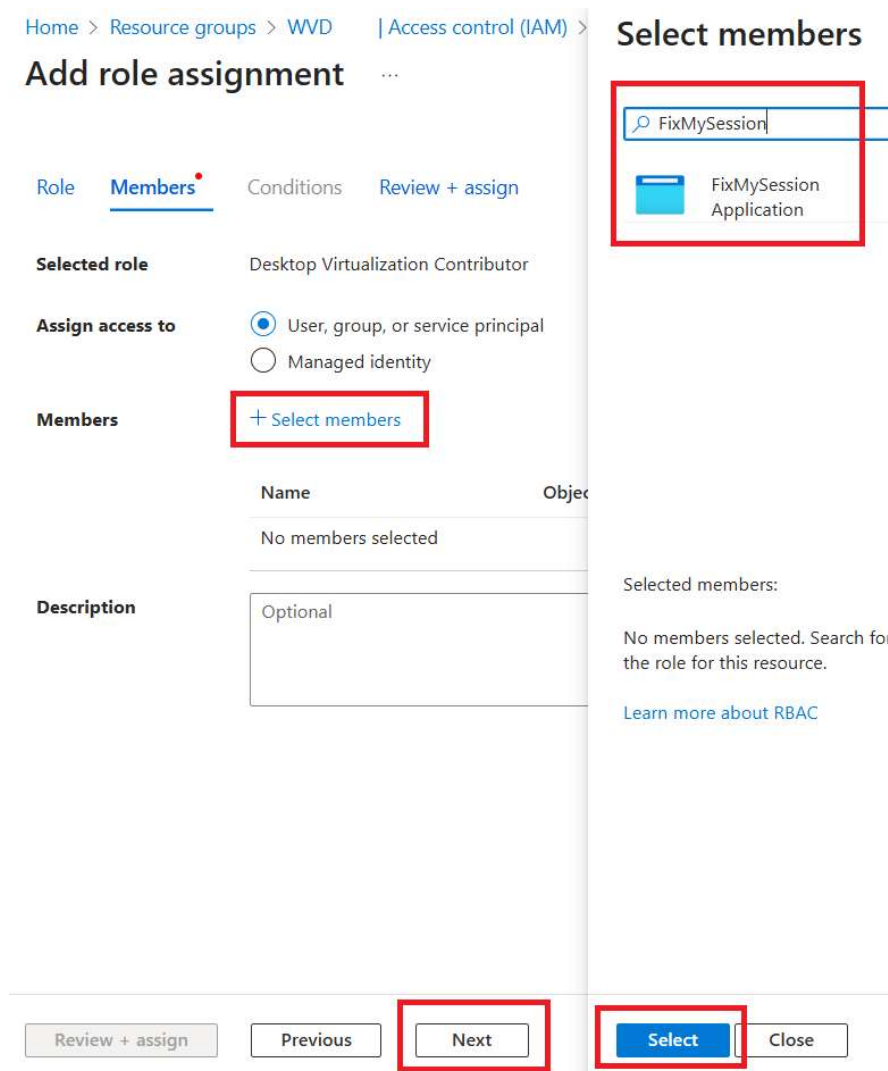
 Type: All

Name ↑↓	Description ↑↓	1
Desktop Virtualization App Attach Contr...	Provide permission to manage app att...	E
Desktop Virtualization Application Grou...	Contributor of the Desktop Virtualizati...	E
Desktop Virtualization Contributor	Contributor of Desktop Virtualization.	E
Desktop Virtualization Host Pool Contr...	Contributor of the Desktop Virtualizati...	E
Desktop Virtualization Power On Contr...	Provide permission to the Azure Virtu...	E
Desktop Virtualization Power On Off Co...	Provide permission to the Azure Virtu...	E
Desktop Virtualization Virtual Machine ...	This role is in preview and subject to c...	E
Desktop Virtualization Workspace Contr...	Contributor of the Desktop Virtualizati...	E

Showing 1 - 8 of 8 results.

[Review + assign](#) [Previous](#) [Next](#)

In the Add Role Assignment area, click "+Select Members." Then type the name of the App Registration you created in Step 1, select it, and click "Select." Finally, click "Next."



Home > Resource groups > WVD | Access control (IAM) > Select members

### Add role assignment

Role **Members** Conditions Review + assign

**Selected role** Desktop Virtualization Contributor

**Assign access to**  User, group, or service principal  Managed identity

**Members** **+ Select members**

Name	Object ID
No members selected	

**Description** Optional

Selected members:

No members selected. Search for the role for this resource.

[Learn more about RBAC](#)

Review + assign Previous **Next** **Select** Close

Finally, click Review and Assign.

Add role assignment ...

[Role](#) [Members](#) [Conditions](#) [Review + assign](#)

**Role** Desktop Virtualization Contributor

**Scope** /subscriptions/5

**Members**

**Name**

FixMySession

**Description**

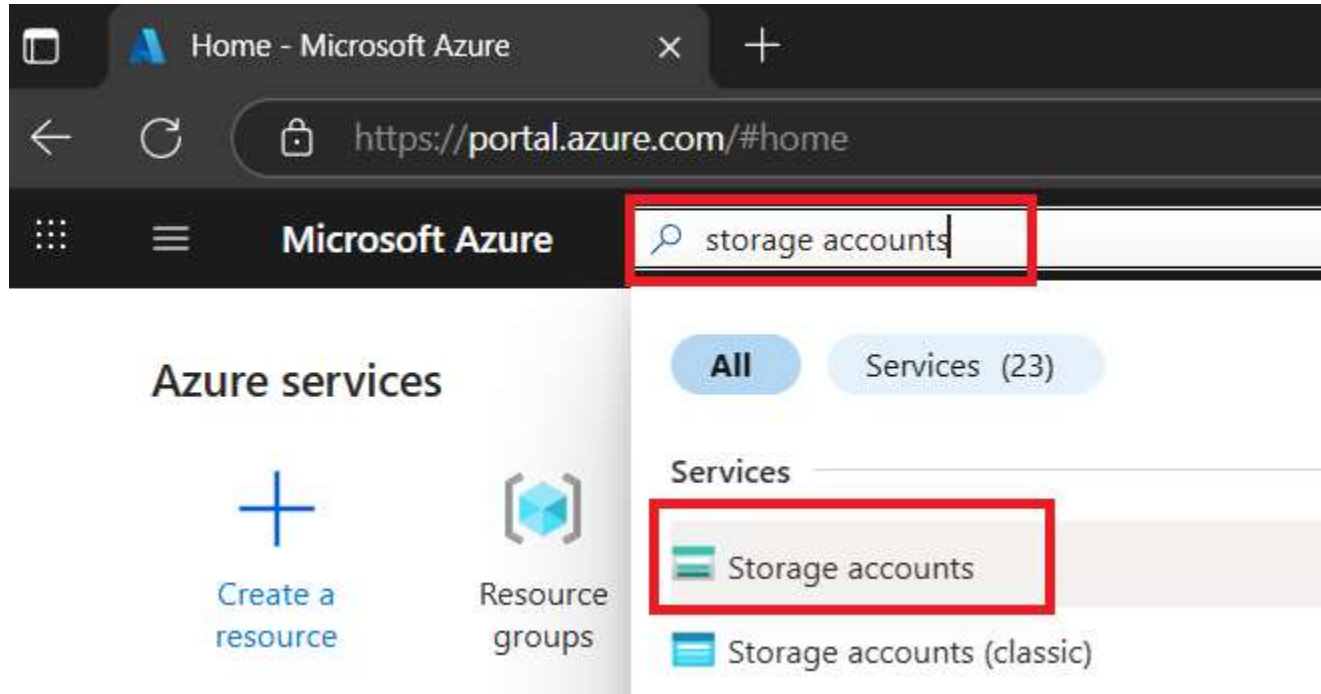
No description

[Review + assign](#)

[Previous](#)

[Next](#)

In the Azure Portal, type "storage accounts" and select it.



Type the name of the storage account that houses the Azure File Shares that host your FSLogix or UPD profile disks, and select it.

## Storage accounts

Default Directory

[+](#) Create [↶](#) Restore [⚙](#) Manage view [∨](#) [↻](#) Refresh [↓](#) Export to CSV [🔗](#) Open query

[i](#) You are viewing a new version of Browse experience. [Click here to access the old experience.](#)

wvddata

Subscription equals all

Resource Group equals all

Local



Name ↑

Type

Kind

Resource Gr



 wvddata

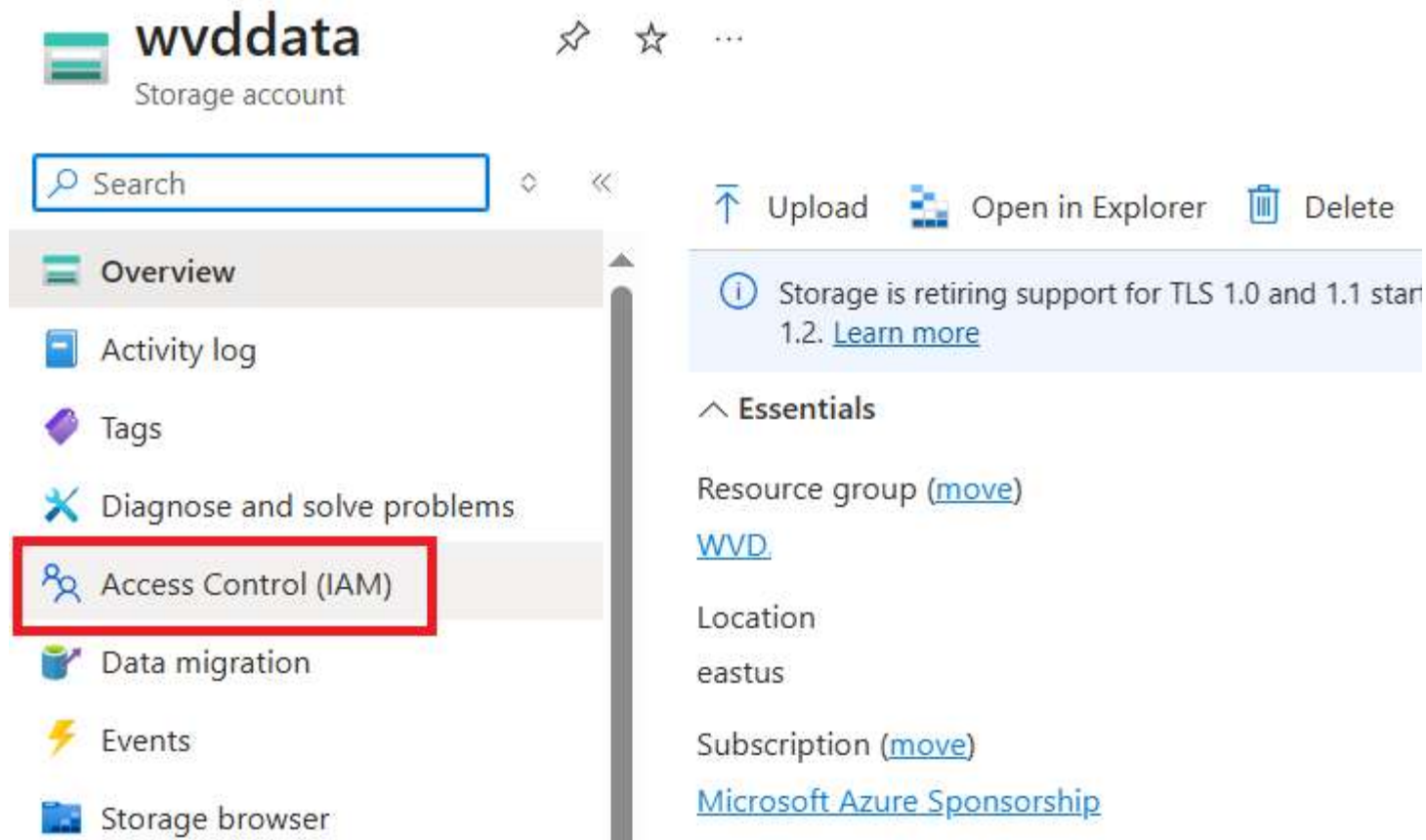


Storage account

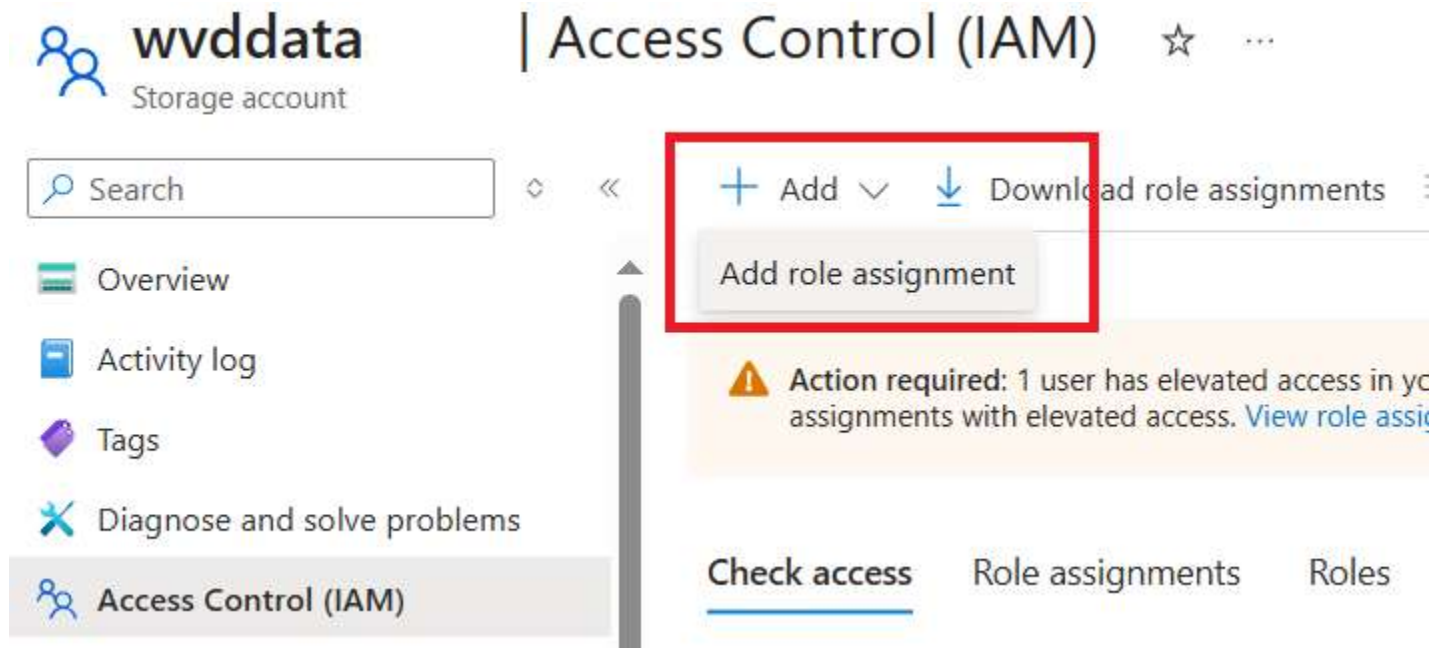
StorageV2

WVD

In the Storage Account blade, click "Access Control (IAM)."



Click on the "+Add" menu to add a role assignment.





**Just as you did for the Desktop Virtualization Contributor Role above, now assign your App Registration role to both the *Storage Account Contributor* role AND the *Storage File Data SMB Share Contributor* roles. You will need to walk through this assignment process twice. Now, your App Registration for the Fix My Session application should have all the permissions it requires to work with Azure File Shares and access host pools and AVD hosts. For the next deployment steps, make sure you have the following information to hand:**

- 1.) Your Azure Subscription ID**
- 2.) The Tenant ID of your AVD Resource Group**
- 3.) The App ID (GUID) of your App Registration / SPN**
- 4.) The App Secret (password) of your App Registration / SPN**
- 5.) The Azure resource group hosting your storage account and AVD host pools**
- 6.) The name of your storage account hosting your FSLogix/UPD file shares, if applicable**
- 7.) The name of your azure file share(s) hosting your FSLogix/UPD profile disks, if applicable**