Azure Meetup Hamburg

Praxisnahes Arbeiten mit Azure Functions, Graph und Managed Identities

Press Space for next page →

Agenda?

- What is a Microsoft managed identity?
- Prerequisites
- Prerequisites VSCode
- Storage Account Explorer & Azurite
- Service Principal Local Deveolpment
- Azure Function App
  - Configure Managed Identity
  - Set Azure Function Graph Permissions
- Start local Function Development
  - Manage local.settings.json
  - Configure requiremnts
  - Run and deploy Azure Function local

Compare Microsoft Azure Managed Identity & Service Principal

Feature	Managed Identity	Service Principal
Description	An Azure service that automatically manages Azure AD identities.	An Azure AD object used to authenticate and authorize applications.
Authentication Mode	Automatically managed by Azure.	Must be manually configured and managed.
Lifecycle Management	Azure automatically manages the lifecycle.	Developers need to manually manage the lifecycle.
Security	Reduced risk as there's no need to store credentials in code or configurations.	Higher risk as credentials need to be managed and securely stored.
Complexity	Easier to use as it requires less manual configuration.	More complex in setup and management.

Prerequisites

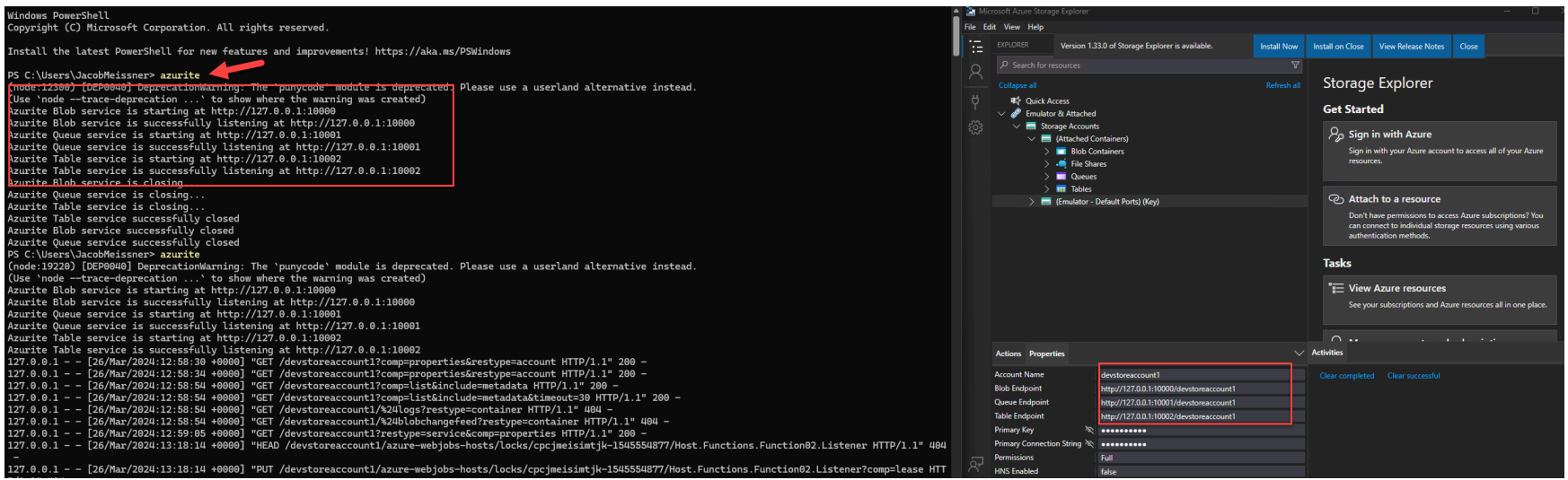
To use Azure Function local Development, some requirements must be fulfilled

- **Storage Explorer** https://azure.microsoft.com/de-de/products/storage/storage-explorer
- **Node JS** https://nodejs.org/en
- **PowerShell 7** https://github.com/PowerShell/PowerShell/releases/download/v7.4.1/PowerShell-7.4.1-win-x64.msi
- **Azurite** 'npm install -g azurite'
- **Azure Function Core Tools** https://go.microsoft.com/fwlink/?linkid=2174087
- VSCode Extensions
  - Azure Tools
  - Azure Functions

Storage Explorer & Azurite

Starting the storage emulator using 'Azurite' in the console or in VSCode

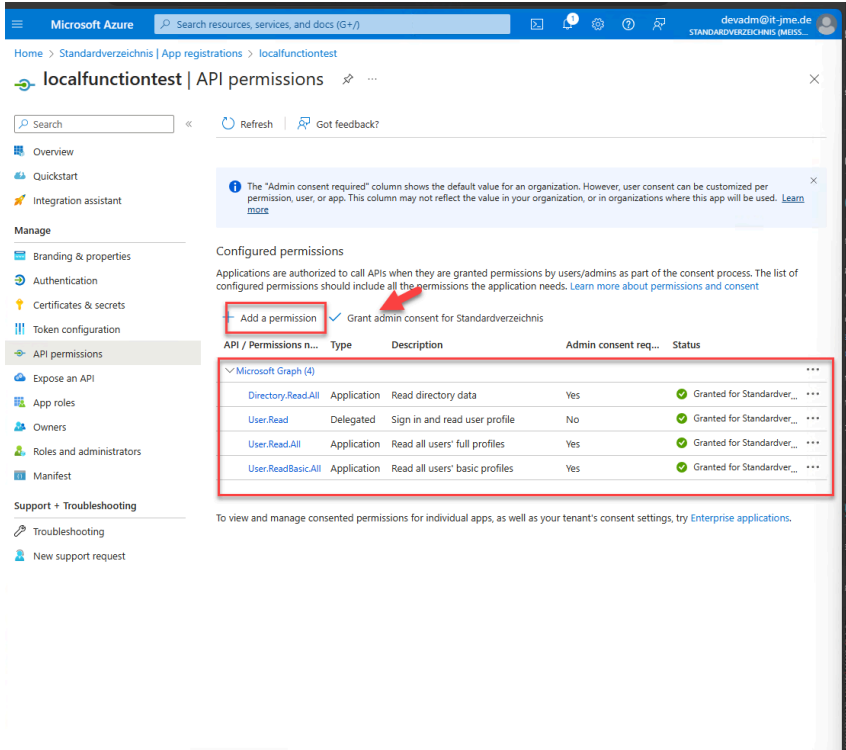
```
Azurite
```

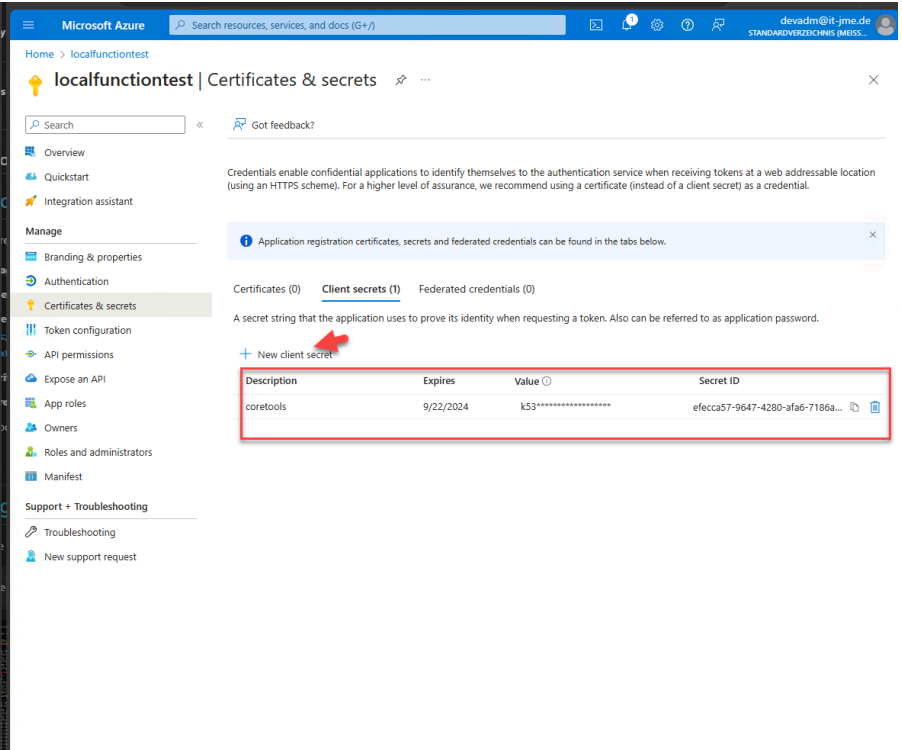


Azure Service Principal

Creating an Azure Service Principal for the local environment

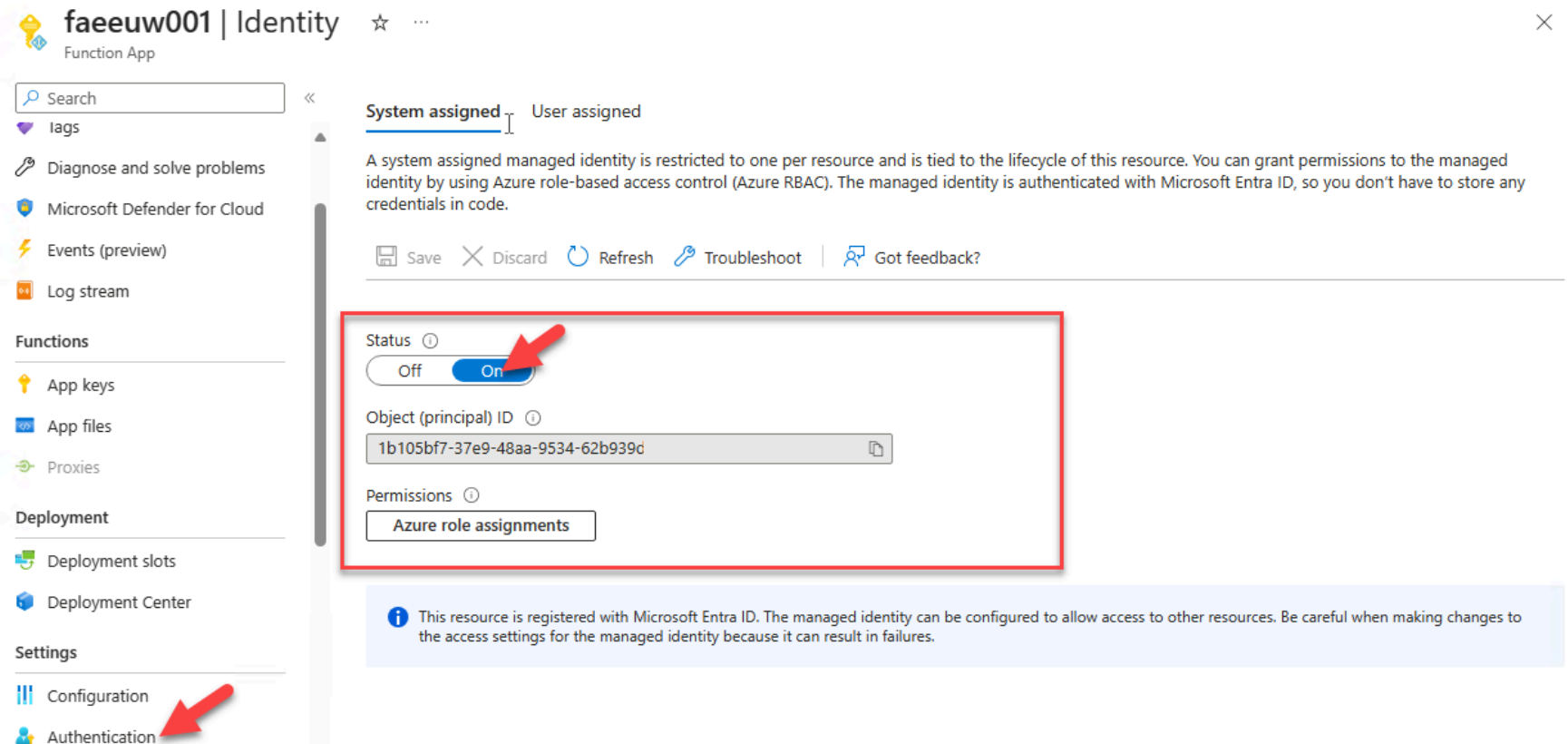
```
New-AzADServicePrincipal -DisplayName "MeinServicePrincipal"
```





Azure Function App & Enable Managed Identity

Create an Azure Function App (e.g. Powershell) and activate the Managed Identity Configuration



Managed Identity Graph Permission

Following the creation of the Managed Identity, the Graph Endpoint must be authorised so that it can access the requested data in the Managed Identity Context.

```
$tenantId = "00000000-0000-0000-0000-000000000000" # Replace with your tenant ID
$graphApiAppId = "00000003-0000-0000-c000-000000000000" # Well known ID
$msiName = "MSINAME" # Name of your managed identity e.g. name of Function or Logic App
$graphPermissions = @("Directory.Read.All", "User.Read.All") # Add or remove permissions

Connect-AzureAD -TenantId $tenantId
$msi = Get-AzureADServicePrincipal -Filter "displayName eq '$msiName'" # Can take a few seconds, add a sleep if necessar
$graphApiAppRegistration = Get-AzureADServicePrincipal -Filter "appId eq '$graphApiAppId'"
$appRoles = $graphApiAppRegistration.AppRoles | Where-Object { $graphPermissions -contains $_.Value -and $_.AllowedMembe
foreach ($appRole in $appRoles) {
  New-AzureAdServiceAppRoleAssignment -ObjectId $msi.ObjectId -PrincipalId $msi.ObjectId -ResourceId $graphApiAppRegistr
}
```

Function Requirements

```
@{
    # For latest supported version, go to 'https://www.powershellgallery.com/packages/Az'. Uncomment the next line and r
    # 'Az' = 'MAJOR_VERSION.*'
    'Az.Accounts' = '2.13.2'
    'PSReadLine' = '2.3.4'
    'Microsoft.Graph.Authentication' = '2.9.0'

}
```