Assigning perms to app registration using Azure AD Authentication

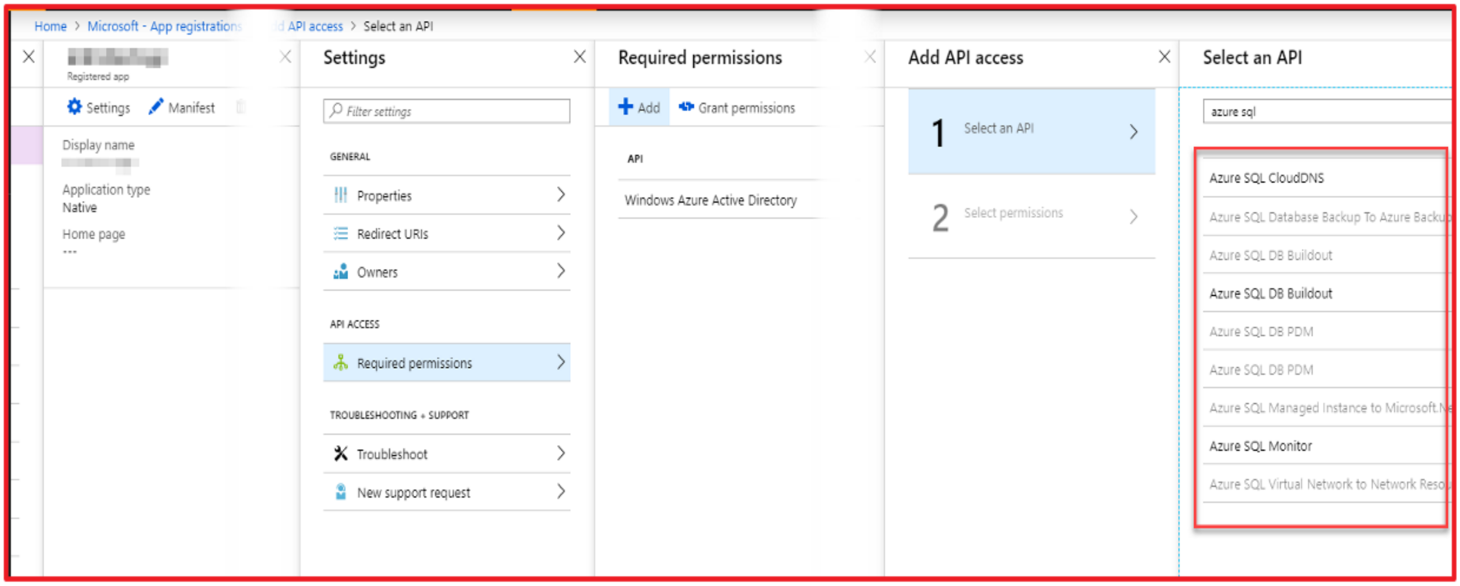
Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Contents

Assigning perms to app registration

Issue

A user is configuring the permissions of an app registration in Azure AD. They are trying to grant access to the "Azure SQL Database" API. "Azure SQL Database" does not appear in the list of available APIs.



[redacted]
Registered app

Display name
[redacted]

Application type
Native

Home page
...

API
Windows Azure Active Directory

1 Select an API
2 Select permissions

azure sql

Azure SQL CloudDNS
Azure SQL Database Backup To Azure Backu
Azure SQL DB Buildout
Azure SQL DB Buildout
Azure SQL DB PDM
Azure SQL DB PDM
Azure SQL Managed Instance to Microsoft.N
Azure SQL Monitor
Azure SQL Virtual Network to Network Reso

Analysis

The missing "Azure SQL Database" entry on the app registration in the Azure Portal is enough to detect the issue. However, if you are in doubt, there are additional steps to further confirm the issue exists, or that it has been resolved.

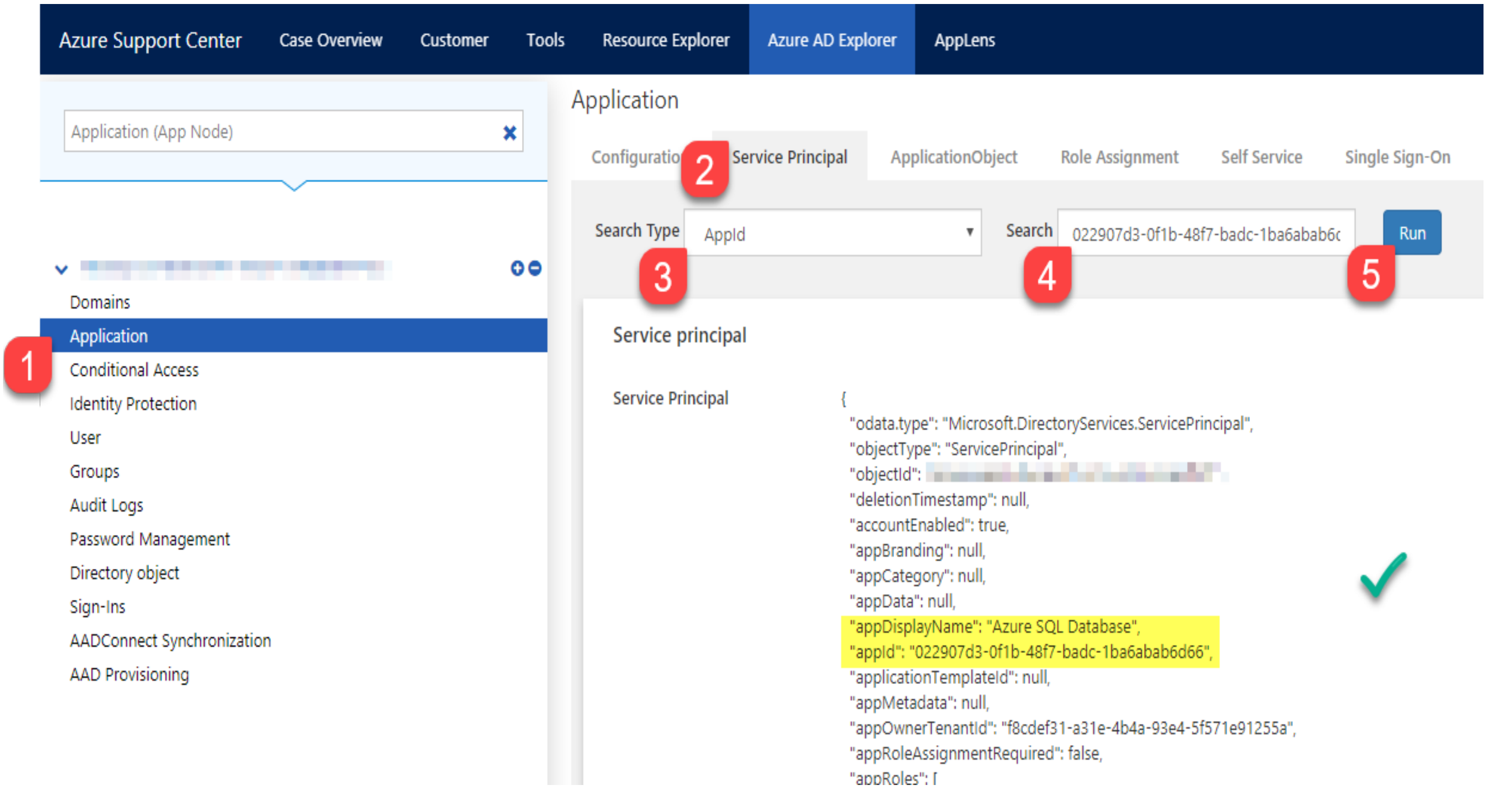
Internal check (using ASC)

Open ASC Azure AD Explorer

1. Select the Application node
2. Select the Service Principal tab
3. Select the AppId search type
4. Insert 022907d3-0f1b-48f7-badc-1ba6abab6d66 in the Search field
5. Click Run

An empty result confirms the issue.

The example below shows a successful query (when the issue is not present).

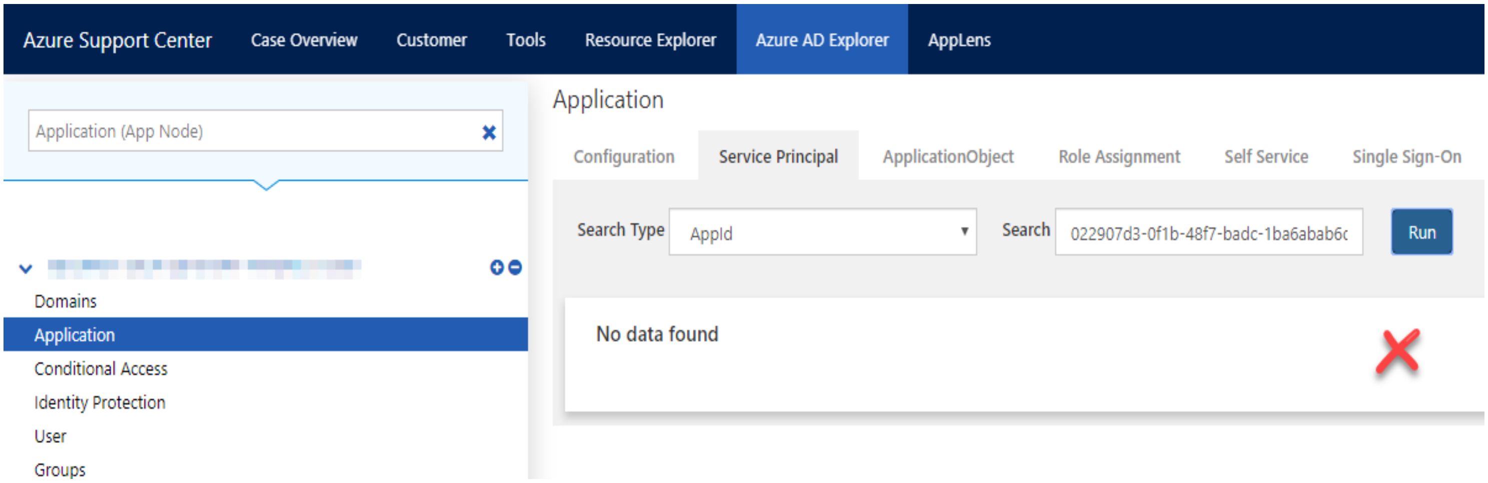


Service principal

Service Principal

```
{
 "odata.type": "Microsoft.DirectoryServices.ServicePrincipal",
 "objectType": "ServicePrincipal",
 "objectId": [redacted]
 "deletionTimestamp": null,
 "accountEnabled": true,
 "appBranding": null,
 "appCategory": null,
 "appData": null,
 "appDisplayName": "Azure SQL Database",
 "appId": "022907d3-0f1b-48f7-badc-1ba6abab6d66",
 "applicationTemplateId": null,
 "appMetadata": null,
 "appOwnerTenantId": "f8cdef31-a31e-4b4a-93e4-5f571e91255a",
 "appRoleAssignmentRequired": false,
 "appRoles": [
```

Here is when the issue is present:



No data found

Check by the customer (querying Azure AD)

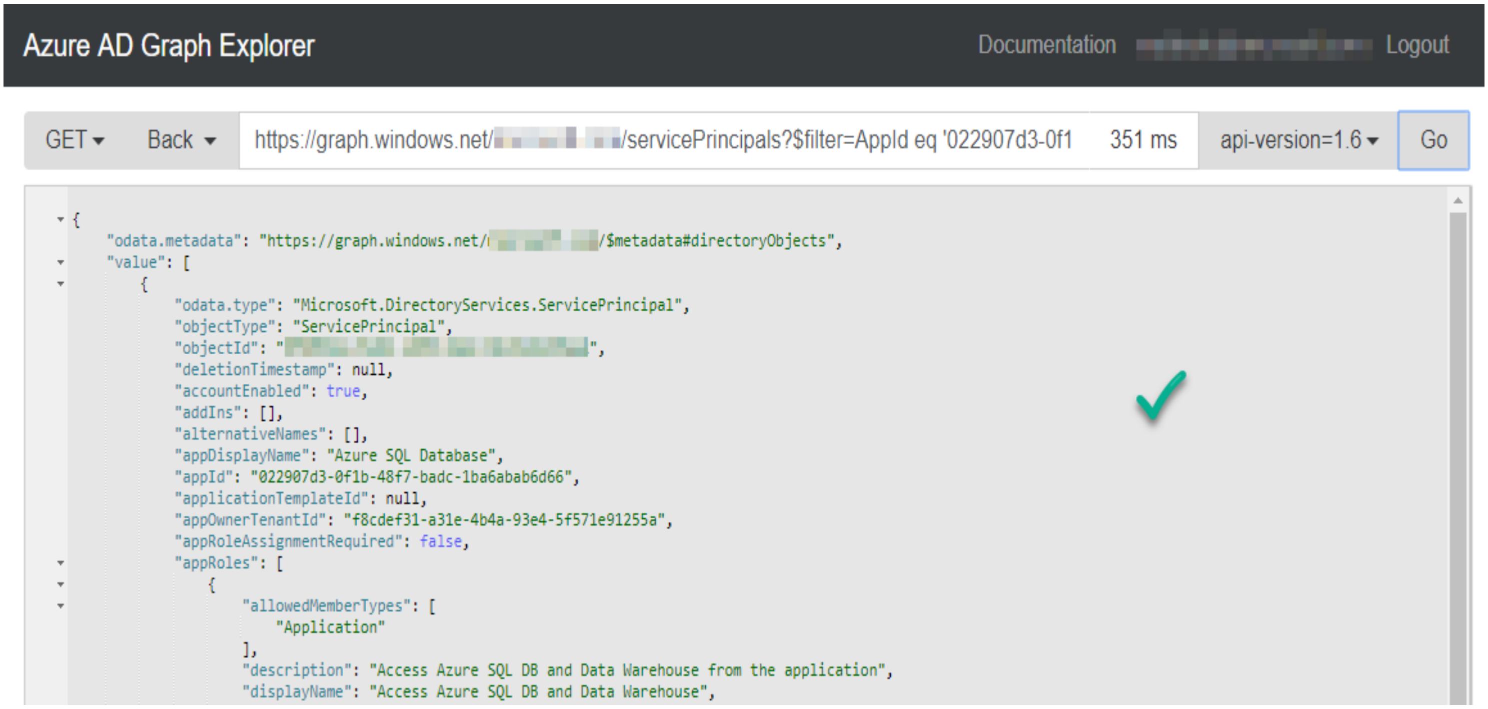
The customer can confirm the issue by querying Azure AD.

1. Open Azure AD Graph Explorer at https://graphexplorer.azurewebsites.net/
2. Login
3. Enter the following query, replacing the tenant with the AAD tenant name (e.g. microsoft.com)
   ```
   https://graph.windows.net/<your tenant="">/servicePrincipals?$filter=AppId eq '022907d3-0f1b-48f7-badc-1ba6abab6d66'
   ```
4. Click Go

If the query returns the following text, the issue is confirmed.

```
{
    "odata.metadata": "https://graph.windows.net/<your tenant="">/$metadata#directoryObjects",
    "value":[ ]
}
```

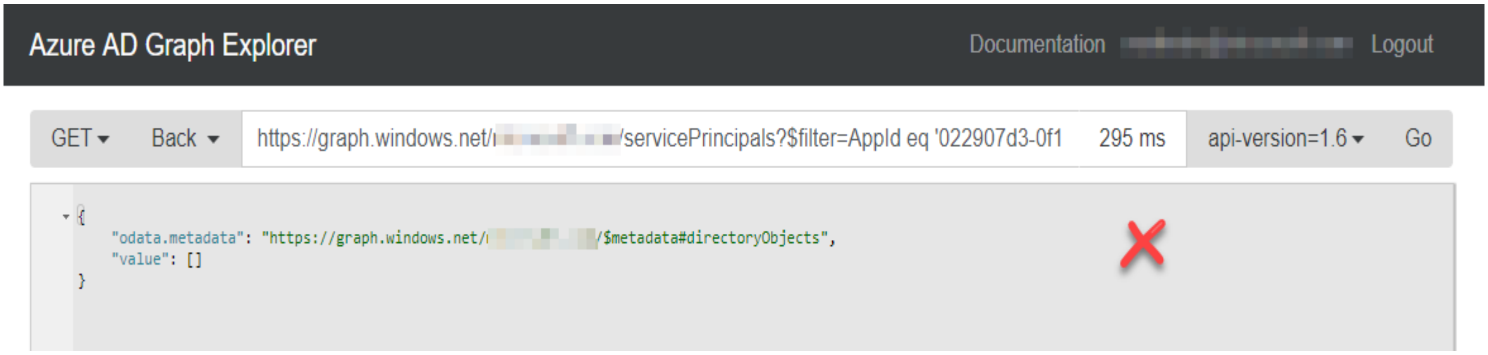
When the issue is not present:



https://graph.windows.net/[redacted]/servicePrincipals?$filter=AppId eq '022907d3-0f1

```
{
    "odata.metadata": "https://graph.windows.net/[redacted]/$metadata#directoryObjects",
    "value": [
        {
            "odata.type": "Microsoft.DirectoryServices.ServicePrincipal",
            "objectType": "ServicePrincipal",
            "objectId": "[redacted]",
            "deletionTimestamp": null,
            "accountEnabled": true,
            "addIns": [],
            "alternativeNames": [],
            "appDisplayName": "Azure SQL Database",
            "appId": "022907d3-0f1b-48f7-badc-1ba6abab6d66",
            "applicationTemplateId": null,
            "appOwnerTenantId": "f8cdef31-a31e-4b4a-93e4-5f571e91255a",
            "appRoleAssignmentRequired": false,
            "appRoles": [
                {
                    "allowedMemberTypes": [
                        "Application"
                    ],
                    "description": "Access Azure SQL DB and Data Warehouse from the application",
                    "displayName": "Access Azure SQL DB and Data Warehouse",
```

When the issue is present:



https://graph.windows.net/[redacted]/servicePrincipals?$filter=AppId eq '022907d3-0f1

```
{
    "odata.metadata": "https://graph.windows.net/[redacted]/$metadata#directoryObjects",
    "value": []
}
```

Resolution

Make sure to have at least one Azure SQL Database logical server configured for Azure AD authentication. If you need to enable Azure AD authentication, please refer to "Configure Azure Active Directory authentication - SQL | Microsoft Docs" (https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure ↗).

1. Connect to Azure SQL Database using the Azure AD administrator (*)
2. Create an Azure AD user with a command like this (specifying a user from your Azure AD tenant).

```
CREATE USER [user@yourtenant.com] FROM EXTERNAL PROVIDER
```

3. Verify that the "Azure SQL Database" API is now available in the permissions of the app registration.

For more information on the steps above you can also refer to step 4 of "Conditional Access - Azure SQL Database and Data Warehouse | Microsoft Docs" (https://docs.microsoft.com/en-us/azure/sql-database/sql-database-conditional-access ↗).

(*) You can connect to Azure SQL Database using the latest version of SQL Server Management Studio. For details please refer to https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure#connect-to-the-user-database-or-data-warehouse-by-using-ssms-or-ssdt ↗.

Additional Reference

The solution is mentioned in step 4 of "Conditional Access - Azure SQL Database and Data Warehouse | Microsoft Docs" (https://docs.microsoft.com/azure/sql-database/sql-database-conditional-access ↗)

The list of APIs available for permissions in app registrations are based on the service principals in the Azure AD tenant (each API listed has a corresponding service principal).

These include the "Azure SQL Database" service principal, with AppId 022907d3-0f1b-48f7-badc-1ba6abab6d66 (note: the AppId for Azure SQL Database is always the same).

The Azure SQL Database service principal is provisioned the first time an Azure AD user is created.

Classification

Root cause Tree - Connectivity/AAD Issue/Other client driver issue

How good have you found this content?

🙂 🙁