

Microsoft identity platform

Developer community call

Microsoft Graph's advanced capabilities for querying directory objects



Luca Spolidoro
Senior Program Manager
lucapol@microsoft.com

May 19th, 2022 | 9:00AM PST / 6:00PM CET

Introduction

- First things first
 - Please note: **We are recording this call** so those unable to attend can benefit from the recording.
 - This call is designed for developers who implement or are interested in implementing Microsoft identity platform solutions.
- What kind of topics will we discuss?
 - We will address development related topics submitted to us by the community for discussion.
 - We build a pipeline of topics for the next few weeks, please submit your feedback and topic suggestions - <https://aka.ms/IDDevCommunityCallSurvey>
 - View recordings on the Microsoft 365 Developer YouTube channel - <https://aka.ms/M365PnP/videos>
 - Follow us on Twitter **@Microsoft365Dev** and **@azuread**
 - This is NOT a support channel. Please use Stack Overflow to ask your immediate support related questions.
- When is the next session?
 - Community Calls: Monthly – 3rd Thursday of every month
 - Next Identity Developer Community Call: June 16th

RECORDING

Microsoft Identity dev community call 19th of May

Download recurrent invite from
<https://aka.ms/IDDevCommunityCalendar>

Microsoft Graph's advanced capabilities for querying directory objects

- Luca Spolidoro (Microsoft)

Agenda

What are the advanced query capabilities?

Under the hood

Query Examples

SDK Support

Conclusion

What are the advanced query capabilities?

\$count, \$filter, \$search, \$orderBy

We added new capabilities to pre-existing [Directory Objects](#) and their links

Object	Navigation Properties
Administrative unit	members
Application	owners
Contact	memberOf, transitiveMemberOf
Device	memberOf, transitiveMemberOf, registeredUsers, registeredOwners
Group	members, transitiveMembers, memberOf, transitiveMemberOf, owners, appRoleAssignments
Service principal	memberOf, transitiveMemberOf, appRoleAssignments, appRoleAssignmentsTo, oAuth2PermissionGrant
User	memberOf, transitiveMemberOf, ownedObjects, registeredDevices, ownedDevices, transitiveManagers, directReports, transitiveReports, appRoleAssignments, oAuth2PermissionGrant
oAuth2PermissionGrant	
transitiveRoleAssignments	

What's your experience with Directory Objects in Microsoft Graph?

Use the chat (pick one):

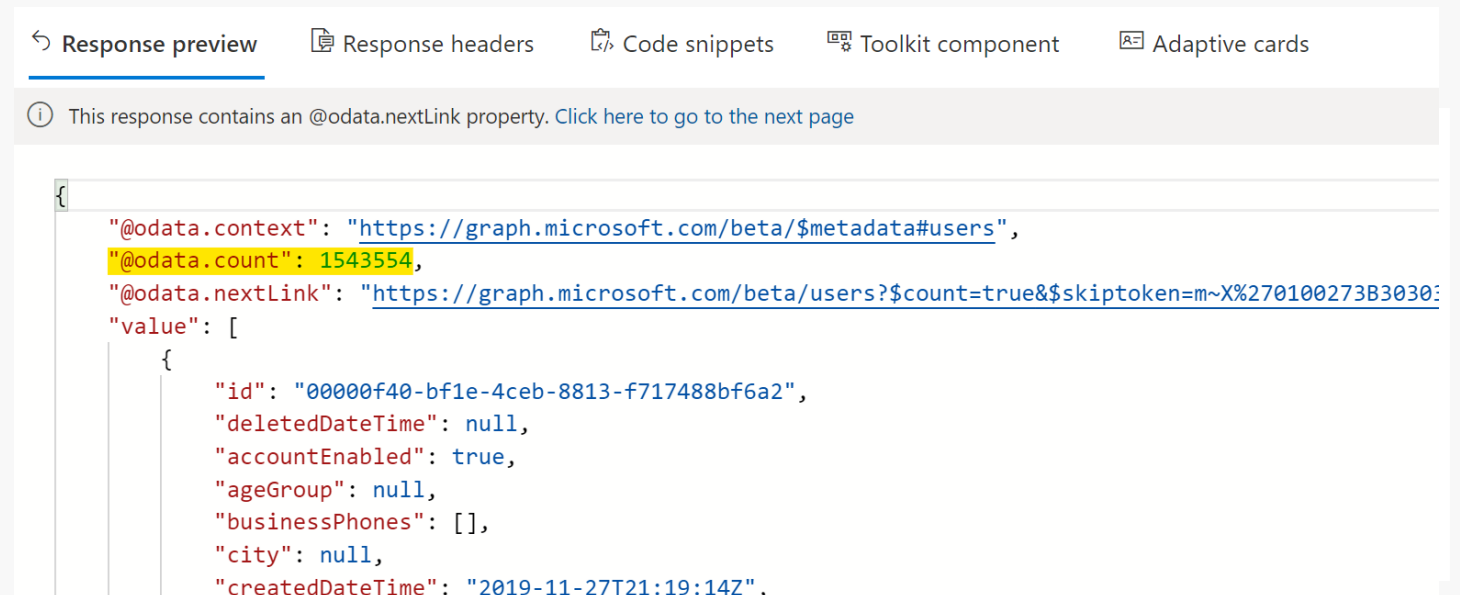
- A. One or more applications in production using it
- B. Built a proof a concept / test app using it
- C. Never used / never heard of it before
- D. Tried it but I was blocked because... (can you tell us why?)

Quick Start

Execute a request using Mezzo Service

1. Go to [Graph Explorer](#)
2. Add Query string
\$count=true
3. Add Request header
ConsistencyLevel=eventual
4. Run the query

Sample Query: [GET](#) `https://graph.microsoft.com/v1.0/users?$count=true`



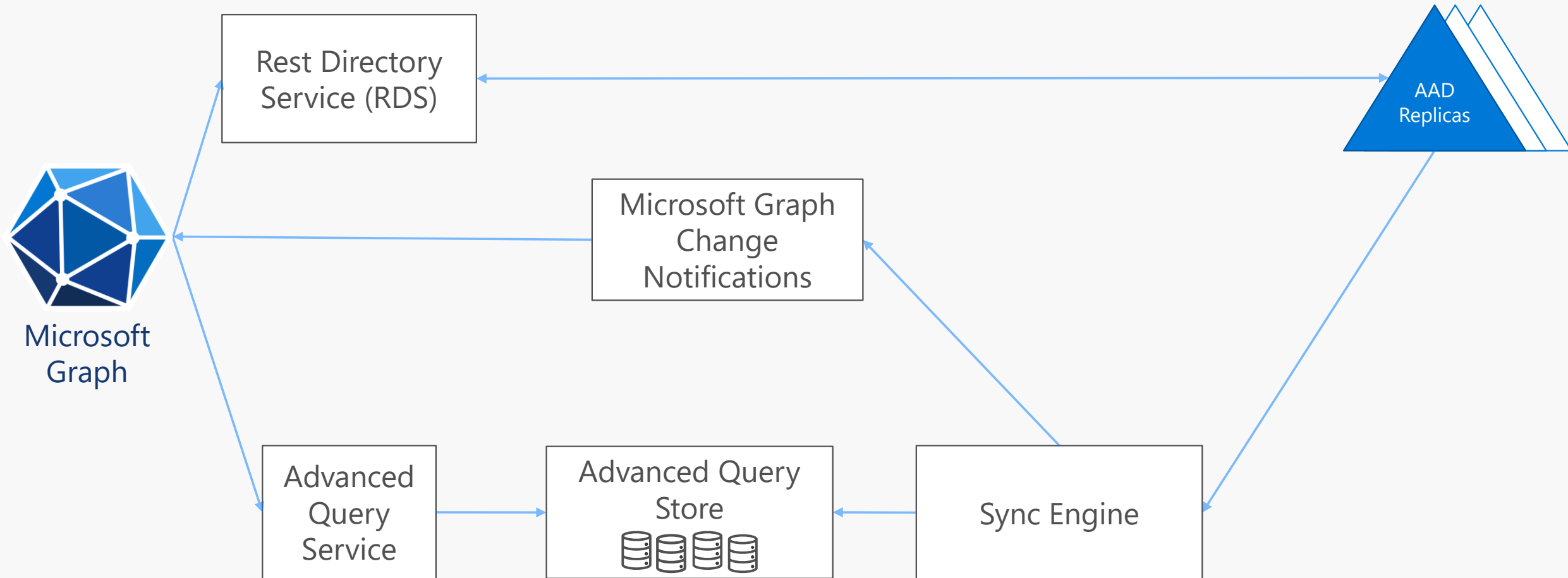
The screenshot shows the 'Response preview' tab in the Mezzo Service interface. It displays the JSON response for a GET request to the Microsoft Graph API. The response includes an @odata.context, an @odata.count of 1543554, and an @odata.nextLink. The 'value' array contains a single user object with various properties like id, deletedDateTime, accountEnabled, ageGroup, businessPhones, city, and createdDateTime.

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#users",
  "@odata.count": 1543554,
  "@odata.nextLink": "https://graph.microsoft.com/beta/users?$count=true&$skiptoken=m~X%270100273B3030:",
  "value": [
    {
      "id": "00000f40-bf1e-4ceb-8813-f717488bf6a2",
      "deletedDateTime": null,
      "accountEnabled": true,
      "ageGroup": null,
      "businessPhones": [],
      "city": null,
      "createdDateTime": "2019-11-27T21:19:14Z",

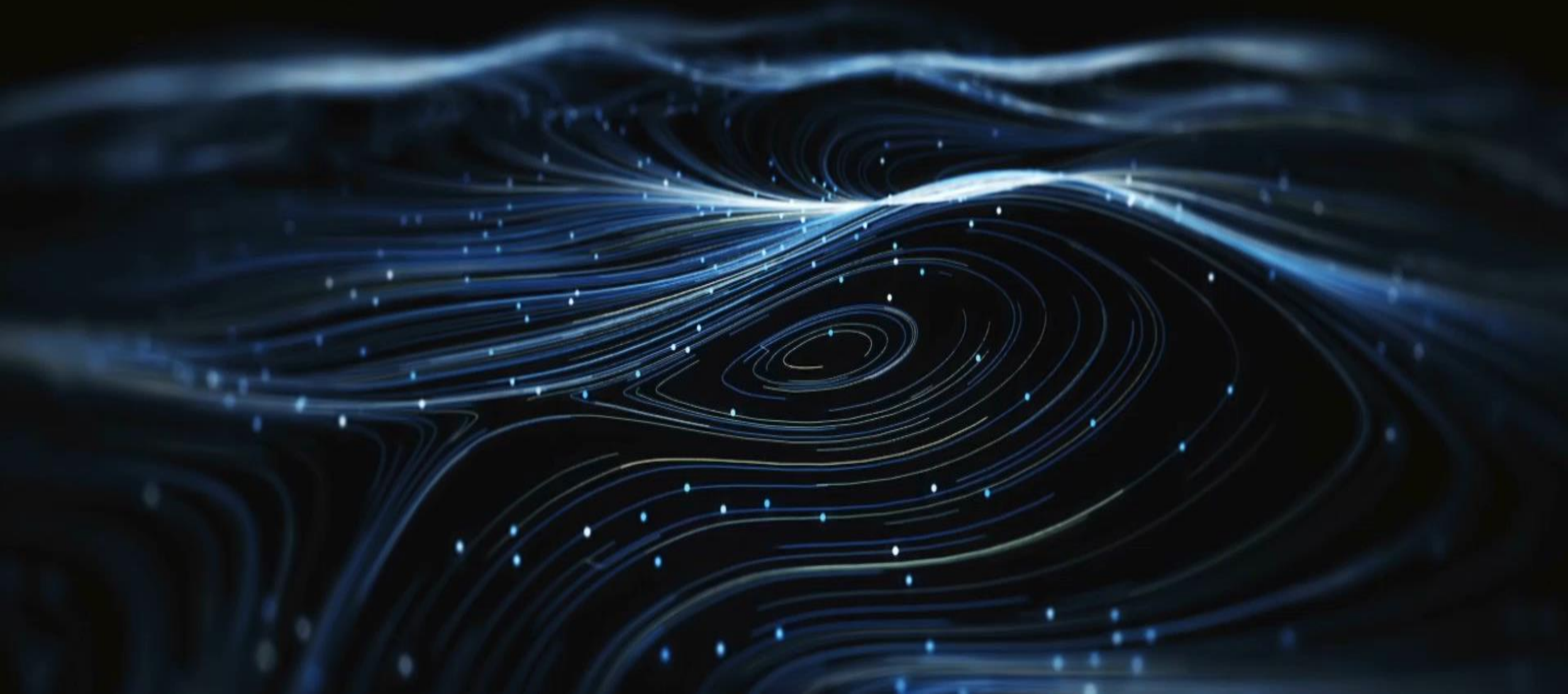
```


Under the hood

From Graph to AAD Store



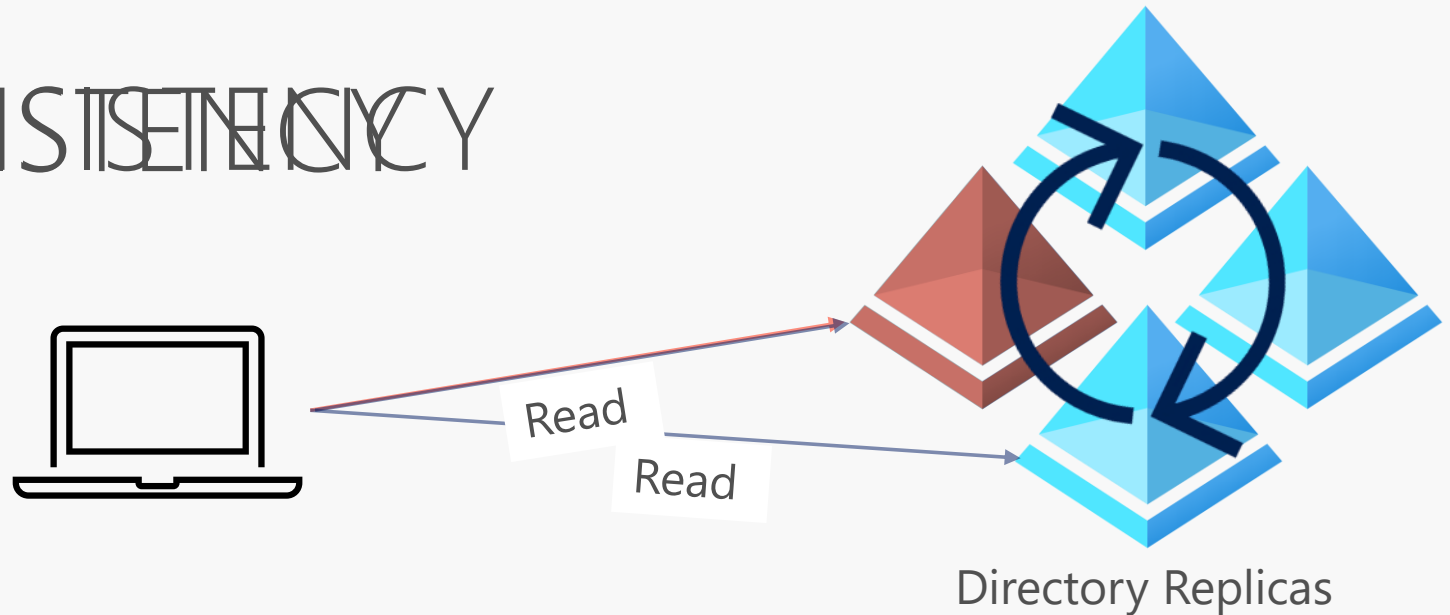
Eventual Consistency



Consistency models in AAD

- ✓ Highly Available
- ✓ Highly Resilient
- ✓ High Performance
- ✓ Multiple servers (replicas)

~~Eventual Consistency~~



Why the magic parameters?



Handling eventual consistency

If	Then
The app is only reading directory data	No issues
The app writes but requires user interaction to read	Use local cache / craft UI to show appropriate messaging
The app writes and automatically reads immediately after	Implement exponential back-off.

Query Examples

Sample Queries – \$Count

Count the number of users, groups, applications, contacts, devices, service principals in a tenant, answering questions like:

- How many users are in the tenant?

[GET https://graph.microsoft.com/beta/users/\\$count](https://graph.microsoft.com/beta/users/$count)

- How many guest users are in the tenant, and who are they?

[GET https://graph.microsoft.com/beta/users/?\\$count=true&\\$filter=userType eq 'Guest'](https://graph.microsoft.com/beta/users/?$count=true&$filter=userType eq 'Guest')

Note: *\$count* can also be a QueryString parameter, returning the count alongside the result set

- How many members are in the engineering group (including transitive and direct members of a group)?

[GET https://graph.microsoft.com/beta/groups/{group-id}/transitiveMembers/\\$count](https://graph.microsoft.com/beta/groups/{group-id}/transitiveMembers/$count)

Note: *A group can contain nested groups, so we are using the transitiveMembers linked property to include all the nested groups' members.*

Sample Queries – \$Search (1/2)

Search terms using tokenization

Note: *tokenized search is currently limited to **displayName** and **description** properties for now.*

*All the other properties default to the **startsWith** behavior.*

*We currently don't offer true substring searches because it will affect the overall search performance: searching for **world** will **not** find **heLLoworLd**.*

Category	Input String	Tokens
Spaces	hello world	hello, world
Different casing	HelloWorld helloWORLD	hello, world
Special characters	hello.world	hello, . , world
Numbers	hello123	hello, 123

- Search for all users in a with "al" in the displayName or with mail *starting with* "admin"

GET [https://graph.microsoft.com/beta/users?](https://graph.microsoft.com/beta/users?$search='displayName:al OR mail:admin')
\$search="displayName:al" OR "mail:admin"

Sample Queries – \$Search (2/2)

- Search for service principals with "sync" in the displayName
[GET https://graph.microsoft.com/beta/servicePrincipals?](https://graph.microsoft.com/beta/servicePrincipals?$count=true&$search='displayName:sync')
[\\$count=true&\\$search="displayName:sync"](https://graph.microsoft.com/beta/servicePrincipals?$count=true&$search='displayName:sync')
- Search transitively in a group for all members with "ra" or "la" in the displayName
[GET https://graph.microsoft.com/beta/groups/{group-id}/](https://graph.microsoft.com/beta/groups/{group-id}/transitiveMembers/microsoft.graph.user/?$count=true&$search='displayName:ra OR displayName:la')
[transitiveMembers/microsoft.graph.user/?](https://graph.microsoft.com/beta/groups/{group-id}/transitiveMembers/microsoft.graph.user/?$count=true&$search='displayName:ra OR displayName:la')
[\\$count=true&\\$search="displayName:ra" OR "displayName:la"](https://graph.microsoft.com/beta/groups/{group-id}/transitiveMembers/microsoft.graph.user/?$count=true&$search='displayName:ra OR displayName:la')

Note: *OData Cast provides a way to trim the results to a specific object type.*

Group members can be of the following types:

User, Application, servicePrincipal, Device.

In the previous example, specifying /microsoft.graph.user in the URL will return only the users in the group.

Sample Queries – Collection \$filter

- Get users by proxyAddress ending with “onmicrosoft.com”:

GET `https://graph.microsoft.com/beta/users?
$count=true&
filter=proxyAddresses/any(p:endsWith(p, 'onmicrosoft.com'))`

Note: all filters can be negated with NOT, including Any(...)

Sample Queries – \$OrderBy

Sorting can be combined with filter or search

- Get last 3 users created that are in building 20:

GET `https://graph.microsoft.com/beta/users?
$count=true&
$orderBy=createddatetime desc&
$filter=startsWith(officelocation, '20')&
$top=3`

Note: **\$count=true** is also required to use **\$orderBy** and **\$filter** together.

Sample Queries – \$Batch

GET \$batch queries require consistency level headers for each request

```
"requests": [  
  {  
    "id": "1",  
    "method": "GET",  
    "url": "/users/$count?$filter=userType eq 'Member'",  
    "headers": {"ConsistencyLevel": "eventual"}  
  },  
  {  
    "id": "2",  
    "method": "GET",  
    "url": "/users/$count?$filter=userType eq 'Guest'",  
    "headers": {"ConsistencyLevel": "eventual"}  
  }  
]
```

SDK Support

PowerShell support

The Microsoft Graph PowerShell SDK is a collection of PowerShell modules that contain cmdlets for calling Microsoft Graph.

```
PowerShell 7 Preview
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS C:\Users\luca> Connect-Graph -Scopes "User.Read.All", "Group.Read.All"
Welcome To Microsoft Graph!
PS C:\Users\luca> Get-MgUser
```

Id	DisplayName	Mail	UserPrincipalName
61254dde-a7a9-4379-bba0-d945644dbe75	Adele Vance	AdeleV@lucaspol.onmicrosoft.com	AdeleV@lucaspol.o...
122604ba-9905-4158-940f-d6765ecafb48	Luca Spolidoro	admin@lucaspol.onmicrosoft.com	admin@lucaspol.on...
33682fd7-c873-4b89-b948-bec2999997ef	Alex Wilber	AlexW@lucaspol.onmicrosoft.com	AlexW@lucaspol.on...
c248a6f4-70f0-4961-b4b7-ff1f108b9a59	Diego Siciliani	DiegoS@lucaspol.onmicrosoft.com	DiegoS@lucaspol.o...
012d9656-3833-48ec-bfd5-4c04a57dbc82	Grady Archie	GradyA@lucaspol.onmicrosoft.com	GradyA@lucaspol.o...
e03d1629-e6e7-4495-b091-c9faf24be1c6	Henrietta Mueller	HenriettaM@lucaspol.onmicrosoft.com	HenriettaM@lucasp...
c7d91845-d36d-4ecc-acf0-9ecb0b0d8c6e	Isaiah Langer	IsaiahL@lucaspol.onmicrosoft.com	IsaiahL@lucaspol. ...
b14dd812-eb9c-4eba-a36d-4089d9cf3bad	Johanna Lorenz	JohannaL@lucaspol.onmicrosoft.com	JohannaL@lucaspol...
e9d461da-d60c-4f21-adac-6bea850b00f7	Joni Sherman	User_252469829598790@lucaspol.onmicrosoft.com	JoniS@lucaspol.on...
b9dfc098-c044-49a0-b153-016a26cd38c7	Lee Gu	LeeG@lucaspol.onmicrosoft.com	LeeG@lucaspol.onm...
6bb19d7e-450f-471d-9ade-76245fddebfb	Lidia Holloway	LidiaH@lucaspol.onmicrosoft.com	LidiaH@lucaspol.o...
55282ecc-83dc-485d-acf2-c47d415ffae8	Lynne Robbins	LynneR@lucaspol.onmicrosoft.com	LynneR@lucaspol.o...
234889ab-d1c9-4120-9524-737417b90130	Megan Bowen	MeganB@lucaspol.onmicrosoft.com	MeganB@lucaspol.o...
4b238208-1998-400c-8488-bfbb67221333	Miriam Graham	MiriamG@lucaspol.onmicrosoft.com	MiriamG@lucaspol. ...
dffb89020-dd1e-4bd1-95d5-5ab2c89802c7	Nestor Wilke	NestorW@lucaspol.onmicrosoft.com	NestorW@lucaspol. ...
4e0f7976-8198-454e-8486-01744bc69448	Patti Fernandez	PattiF@lucaspol.onmicrosoft.com	PattiF@lucaspol.o...
d25182dd-788c-428c-909f-0b6b63d7d590	Pradeep Gupta	PradeepG@lucaspol.onmicrosoft.com	PradeepG@lucaspol...

```
PS C:\Users\luca> |
```

MSGraph PowerShell Quick start

1. Install [Windows Terminal](#) (optional)
2. Install [PowerShell Core](#)
3. `Install-Module Microsoft.Graph`
4. `Import-Module Microsoft.Graph.Authentication`
5. `Import-Module Microsoft.Graph.Users.User`
6. `Get-Command -Module Microsoft.Graph*`
7. `Connect-Graph -Scopes "User.Read.All"`
8. `Get-mgUser -ConsistencyLevel eventual
-Count UserCount
-Search '"displayName:room"'`

.NET SDK

MsGraph Samples

Select

id, displayName, mail, userPrincipalName

Filter

displayName ne 'Luca Spolidoro'

Order By

displayName

Search

Entities (34)

Users

Load

https://graph.microsoft.com/v1.0/users?\$count=true&\$filter=displayName ne 'Luca Spolidoro'&\$orderBy=displayName&\$select=id, displayName, mail, userPrincipalName

Graph Explorer

DisplayName	Mail	UserPrincipalName	Id
Adele Vance	AdeleV@M365x351100.OnMicrosoft.com	AdeleV@M365x351100.OnMicrosoft.com	07a773b6-6635-413c-b51f-71eb3819e9a0
Alex Wilber	AlexW@M365x351100.OnMicrosoft.com	AlexW@M365x351100.OnMicrosoft.com	9090ec45-6e12-449a-bf40-a7ec2f9bf437
Allan Deyoung	AllanD@M365x351100.OnMicrosoft.com	AllanD@M365x351100.OnMicrosoft.com	ae134c0d-07b5-4019-a01f-46f4f2ef3d3b
Automate Bot		AutomateB@M365x351100.OnMicrosoft.com	518ef3e0-0501-4d5e-89e3-2ab8fbb2adf8
Bianca Pisani		BiancaP@M365x351100.OnMicrosoft.com	20c3e8fc-9f67-4dd2-97c6-c36f6da3200d
Brian Johnson (TAILSPIN)	BrianJ@M365x351100.OnMicrosoft.com	BrianJ@M365x351100.OnMicrosoft.com	2588d13b-7b77-40f2-a607-43e1ca2ccd07
Cameron White		CameronW@M365x351100.OnMicrosoft.com	b81f2d70-16d6-4517-9299-124ecbf5d1b6

.NET and other SDKs still need to catch-up, but there are workarounds.
[This sample app](#) will show how to.

Conclusion

Current Limitations

- All these capabilities are **not supported in B2C tenants**
- **\$search** only limited to **displayName** and **description** properties for now, all the other properties default to the **startsWith** behavior.
- **endsWith \$filter** only limited to:
mail, otherMails, userPrincipalName and **proxyAddresses**
- No support for **\$expand** (silently failing)
- No support for **\$skip** (only **\$skipToken**)
- Supports only **Eventual Consistency**

References and Additional Resources

- [Advanced query capabilities on Azure AD directory objects - Microsoft Graph | Microsoft Docs](#)
- <https://github.com/microsoftgraph/dotnet-aad-query-sample>
- To give feedback please fill this survey:
<https://aka.ms/MsGraphAADSurveyComm>



Thank you

Recording will be available soon on the
Microsoft 365 Community (PnP) YouTube channel

<https://aka.ms/M365PnP/videos>

(subscribe today)

Follow us on Twitter

[@Microsoft365Dev](#) and [@azuread](#)

Next call: **June 16th at 9:00am PT**

<https://aka.ms/IDDevCommunityCalendar>

Q&A