



S P E C T E R O P S

It's Raining Shells

How to Find New Attack Primitives in Azure

Permalink to this deck: <https://bit.ly/3ItRi6u>

Hello!

My name is

Andy Robbins

Co-creator of [BloodHound](#)

Product Architect of [BloodHound Enterprise](#)

I work at [@SpecterOps](#)

You can find me at [@ waldo](#)



Agenda

Why abuses, not bugs?

Crash Course Through The Basics

Finding New Attack Primitives: MS Graph Case Study

Where to find research ideas

Conclusion

Agenda

Why abuses, not bugs?

Crash Course Through The Basics

Finding New Attack Primitives: MS Graph Case Study

Where to find research ideas

Conclusion

Abuse primitives:

- Generally enjoy a dramatically longer shelf life

Abuse primitives:

- Generally enjoy a dramatically longer shelf life
- Are much **cheaper to maintain** over time

Abuse primitives:

- Generally enjoy a dramatically longer shelf life
- Are much cheaper to maintain over time
- Exist in almost **every instance** of a given platform

Abuse primitives:

- Generally enjoy a dramatically longer shelf life
- Are much cheaper to maintain over time
- Exist in almost every instance of a given platform
- Present a **notorious challenge** to detection engineers



thaddeus e. grugq

@thegrugq

**Give a man an Oday and he'll have access for a day,
teach a man to phish and he'll have access for life.**

11:35 PM · Feb 6, 2015 · Tweetbot for iOS

5,269 Retweets

211 Quote Tweets

8,877 Likes

<https://twitter.com/thegrugq/status/563964286783877121>



Matt Graeber

@mattifestation

**A sufficiently advanced threat actor is
indistinguishable from a competent system
administrator.**

10:38 AM · Dec 14, 2016 · Twitter Web Client

127 Retweets **11** Quote Tweets **199** Likes

<https://twitter.com/mattifestation/status/809105346870460416>

Agenda

Why Azure abuses?

Crash Course Through The Basics

Finding New Attack Primitives: MS Graph Case Study

Where to find research ideas

Conclusion

What (exactly) is Azure?

Simply put: Azure is Microsoft's cloud computing product.

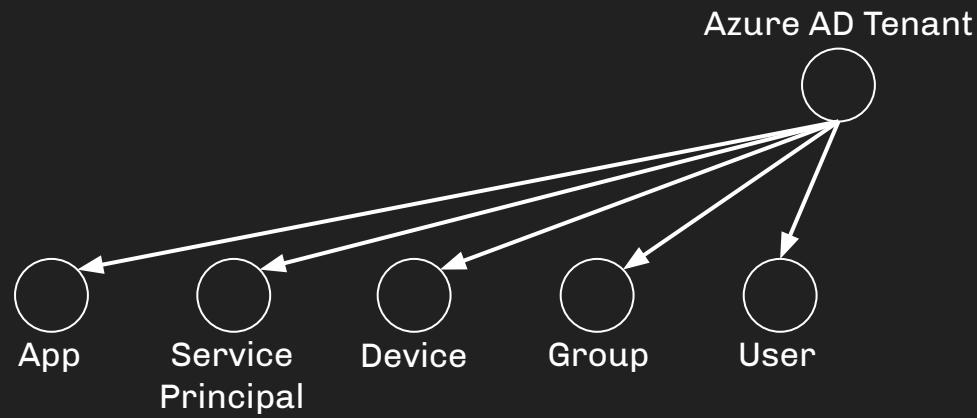
Azure is comprised of more than 600 distinct services that cover:

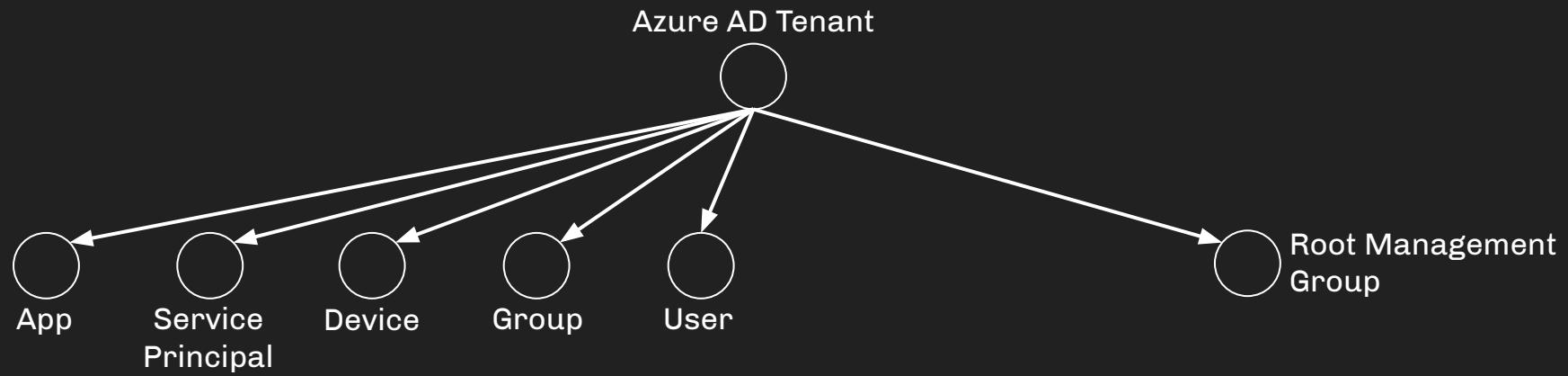
- Identity
- Computing
- Storage
- Data management
- Messaging
- DevOps
- IoT
- etc

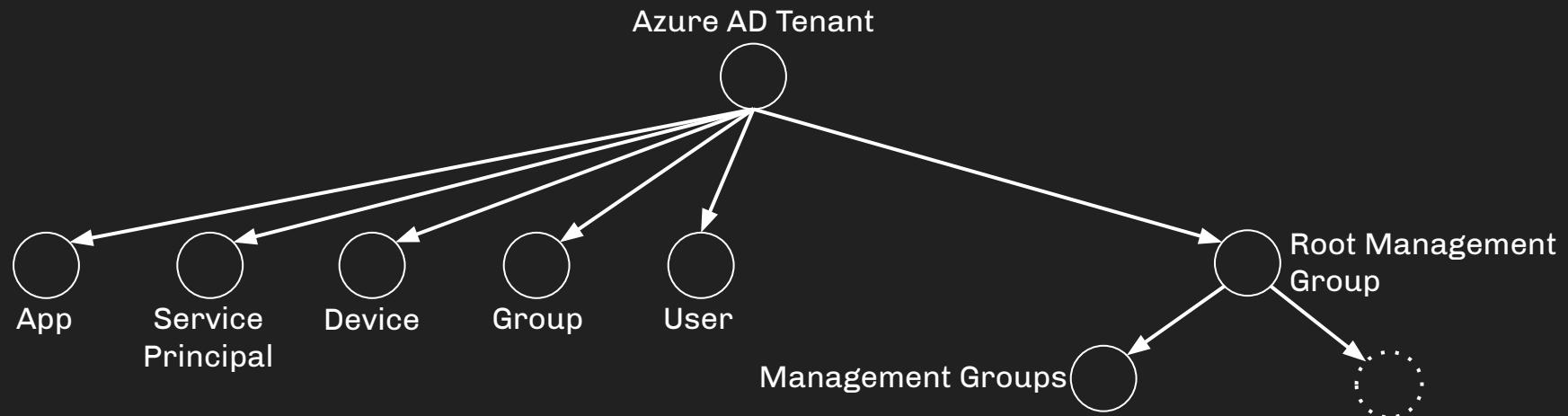
Securable Object Hierarchy

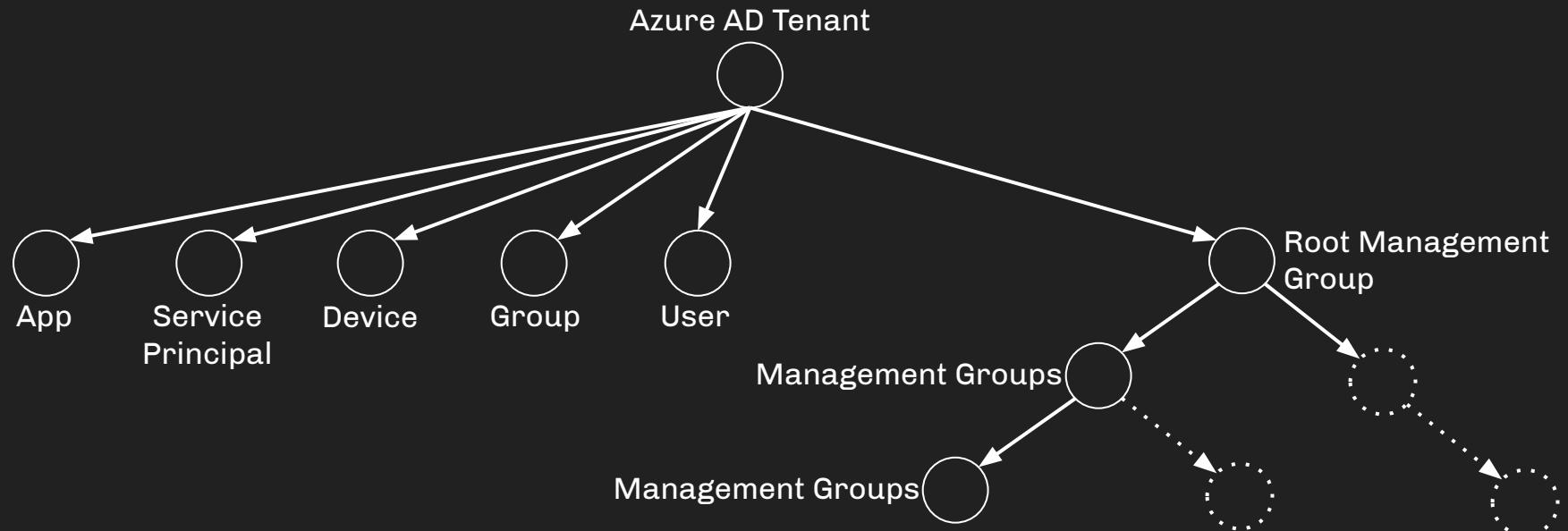
Azure AD Tenant

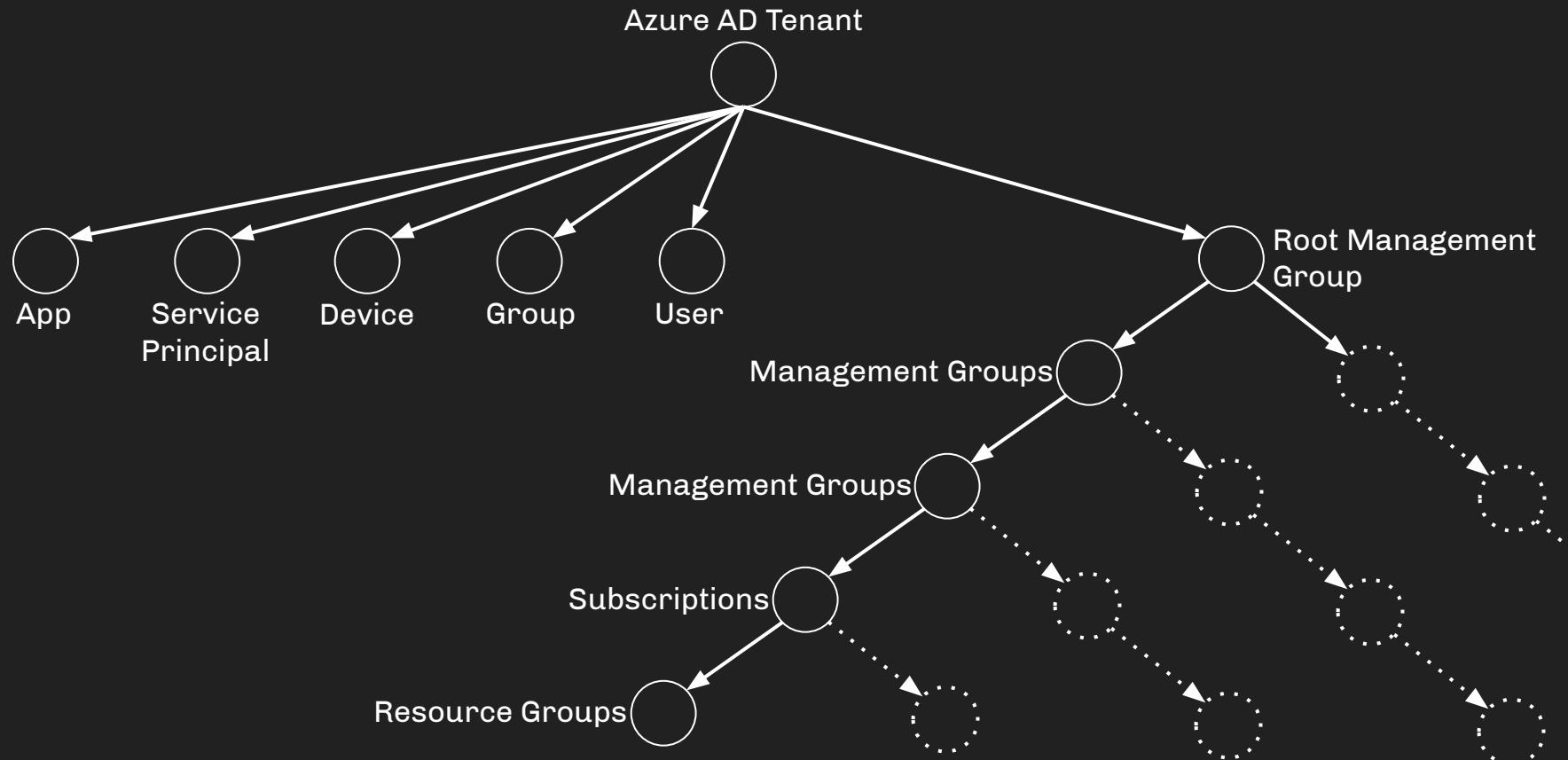


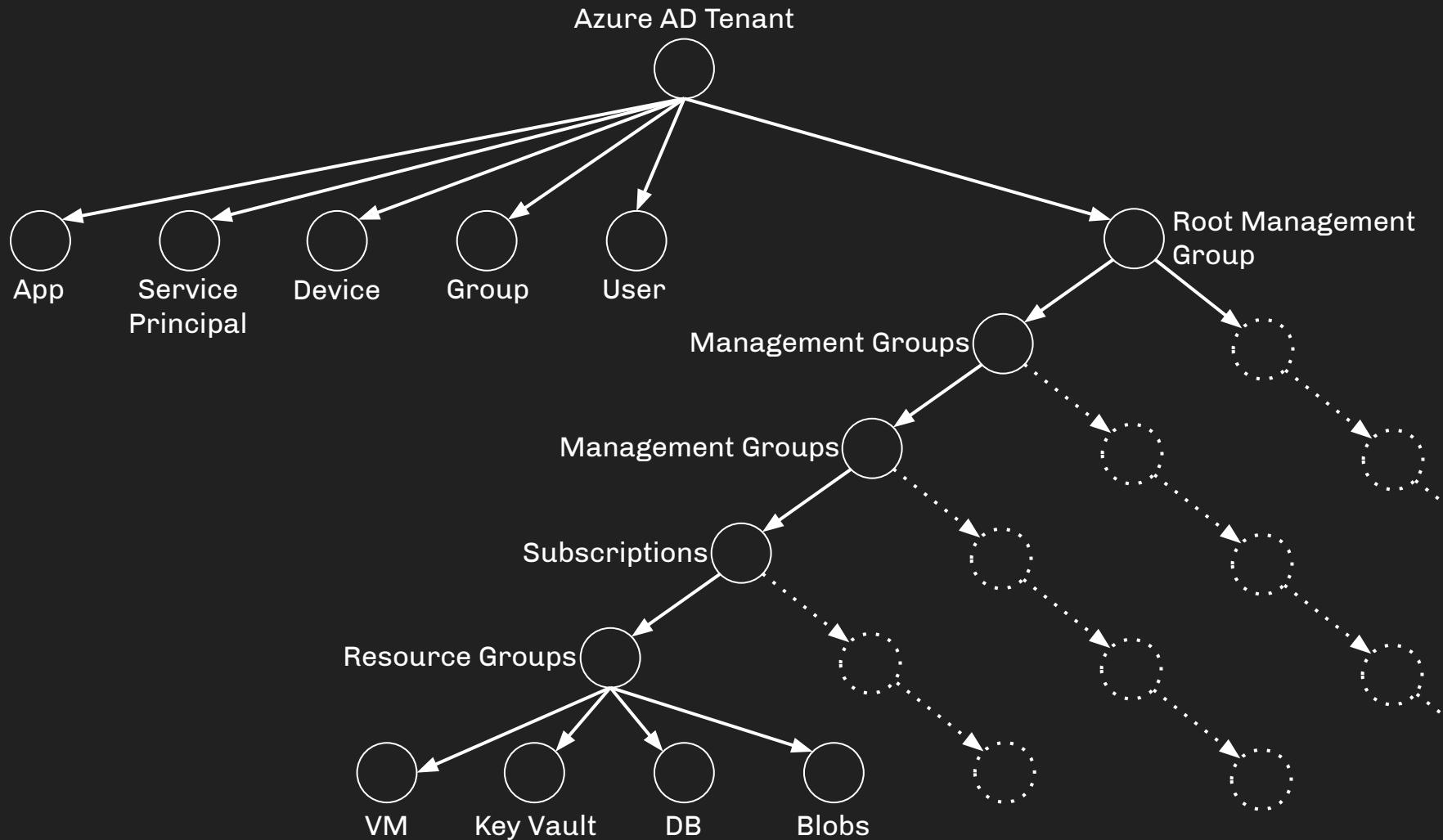




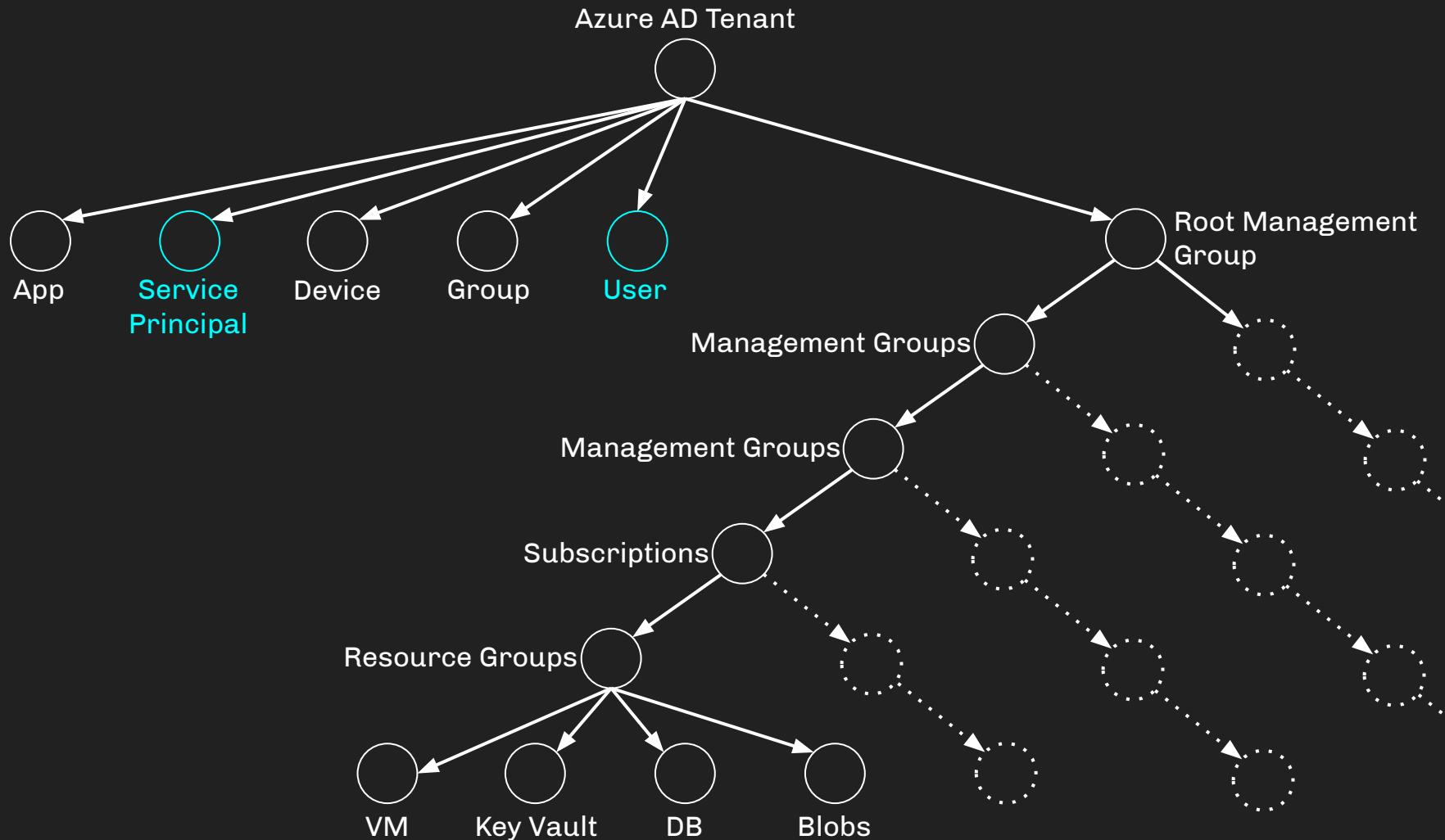




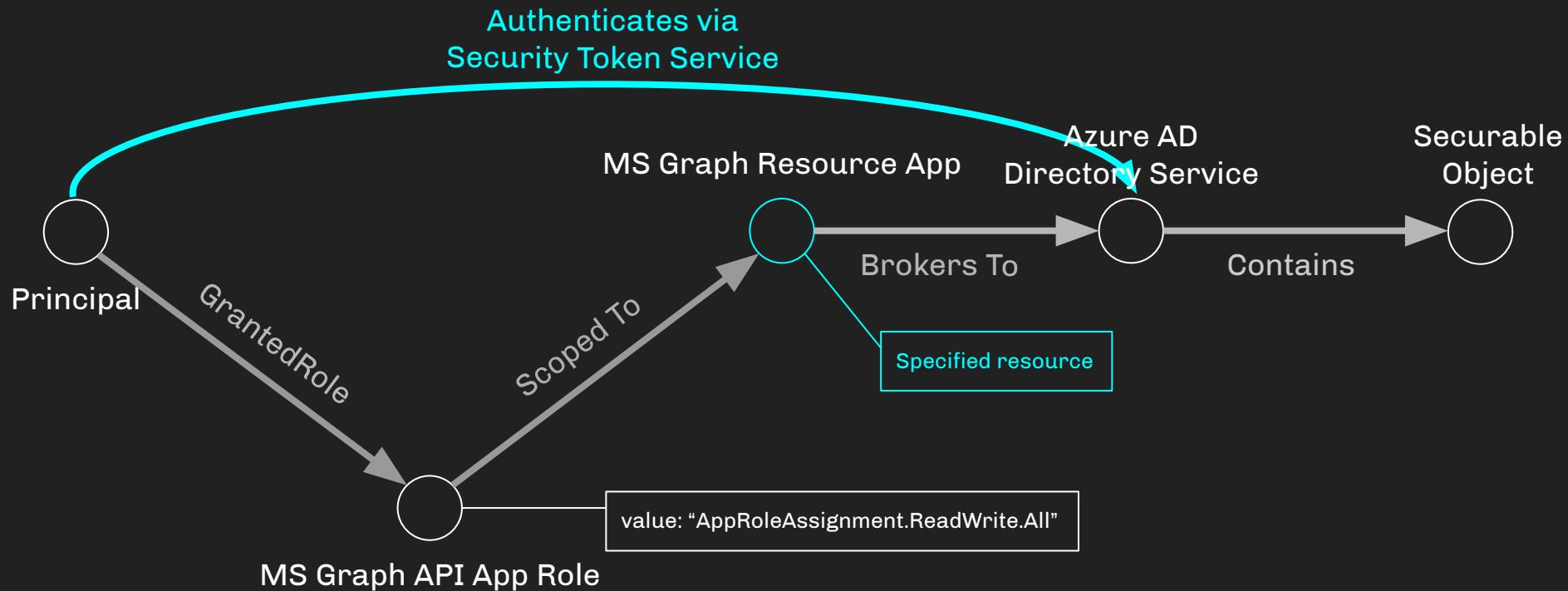




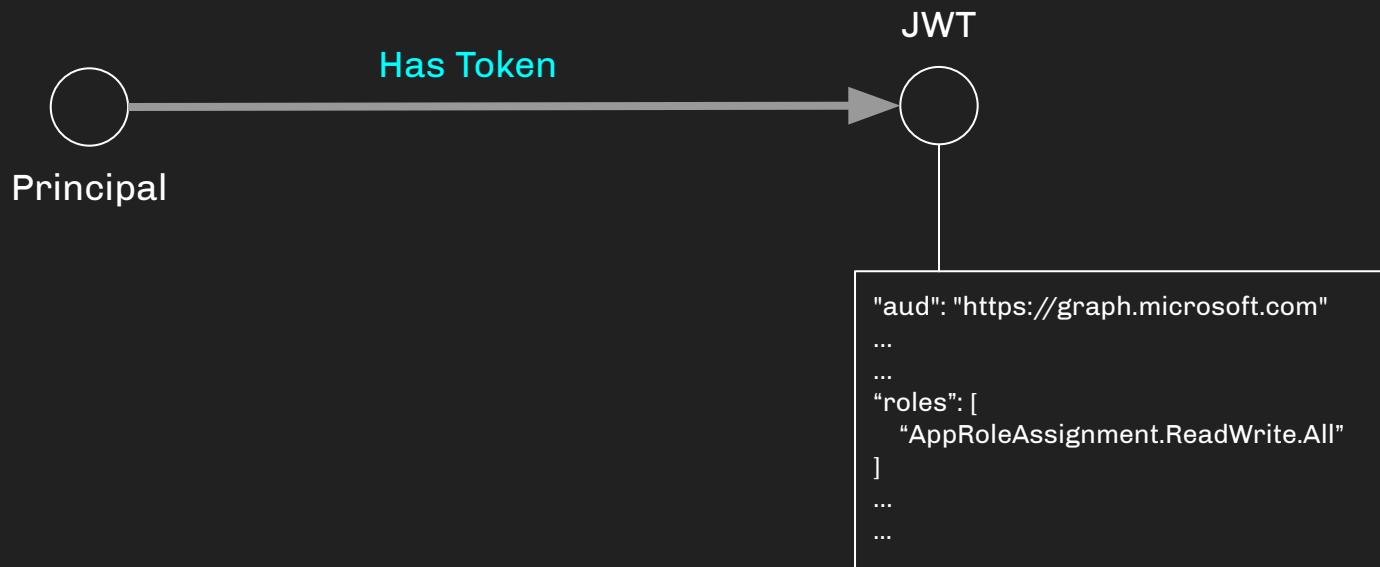
Authentication



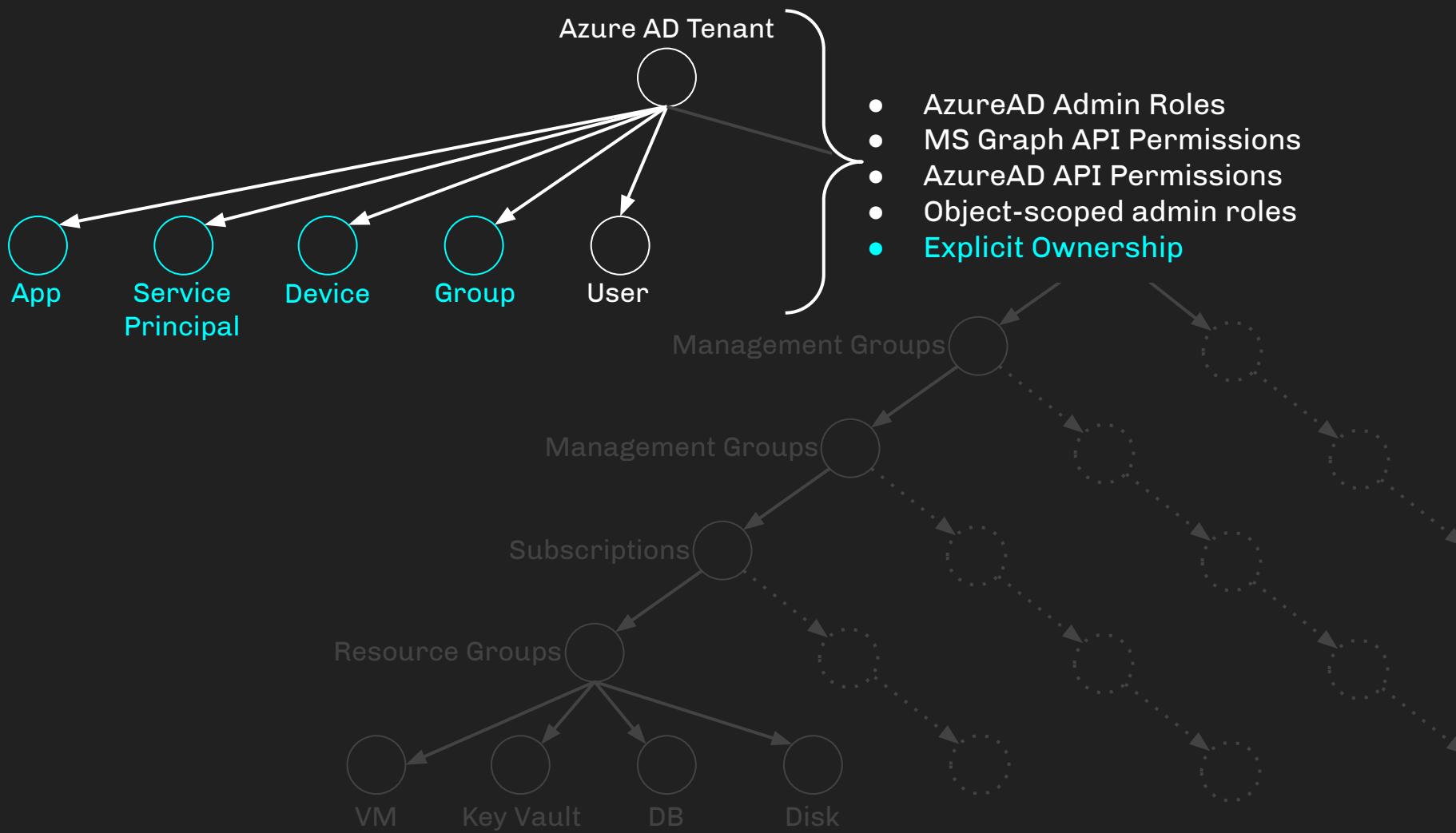
Token issuance

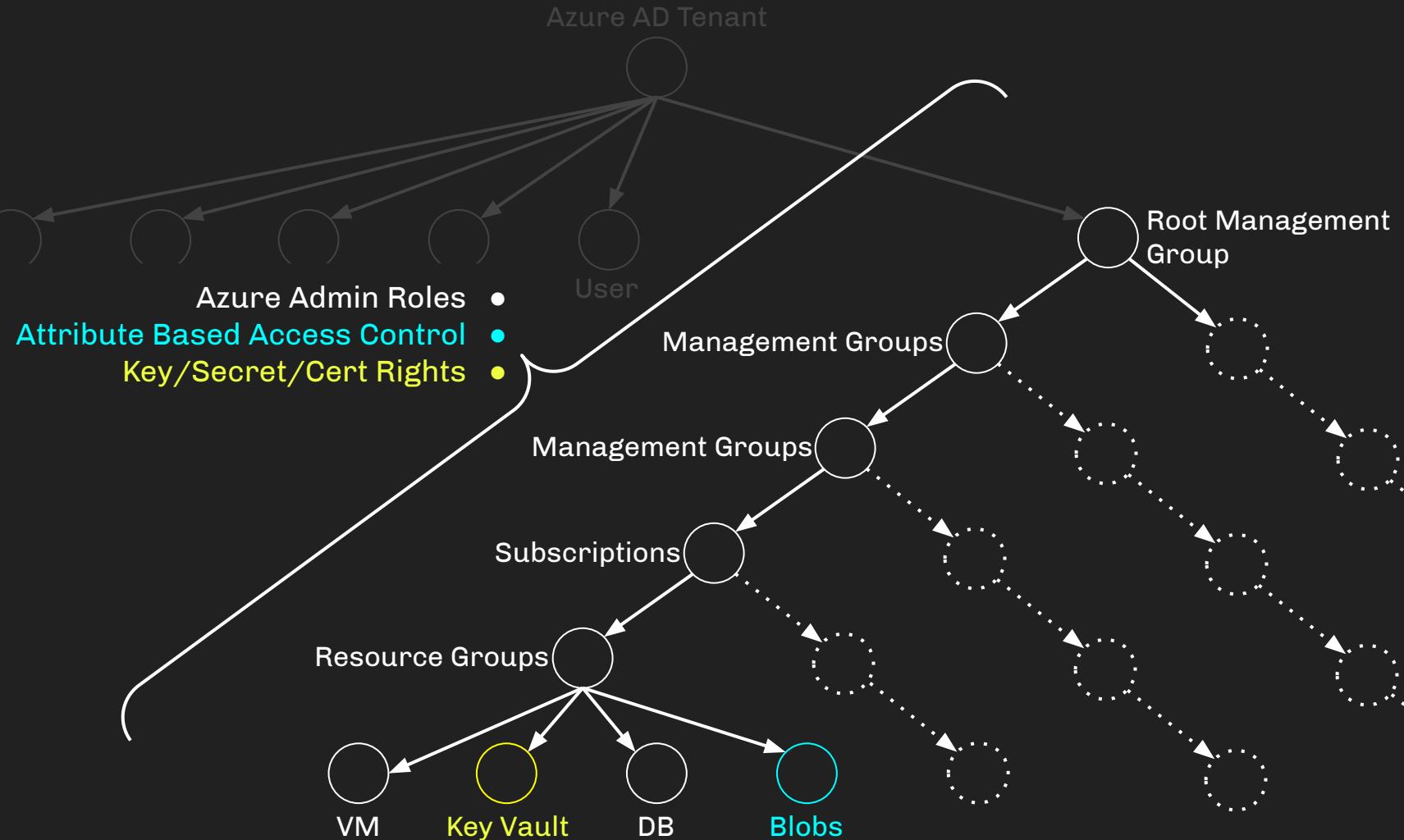


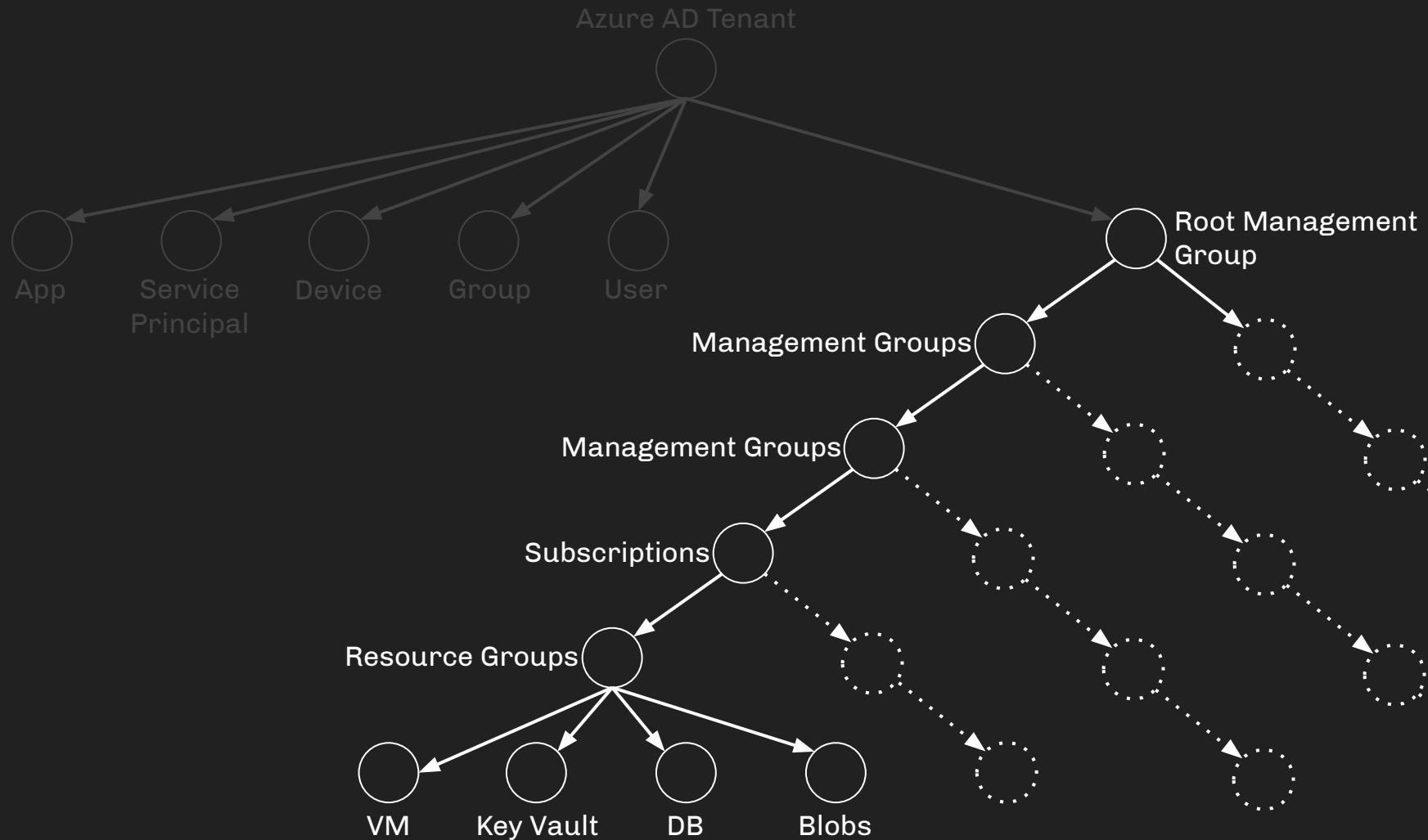
Token issuance

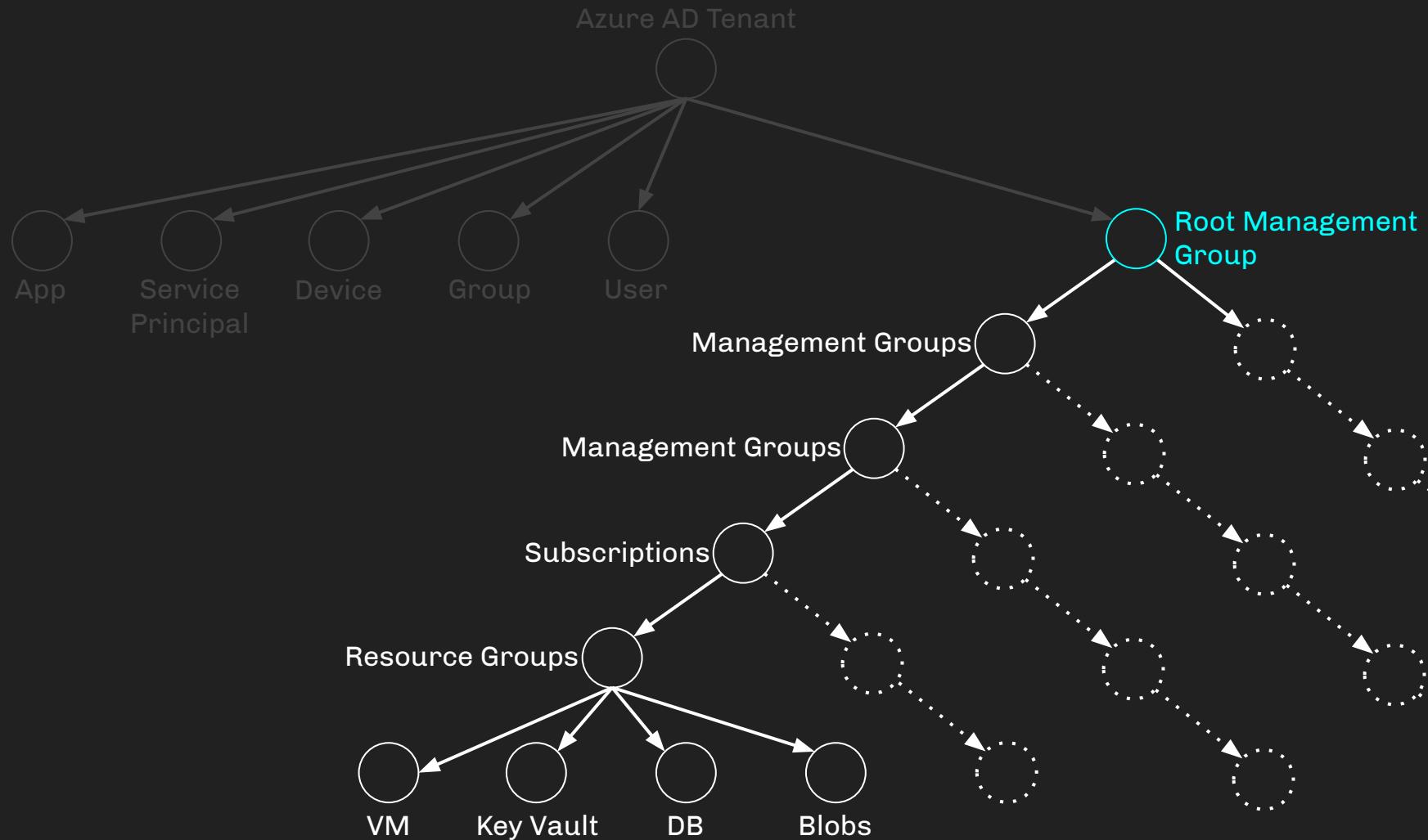


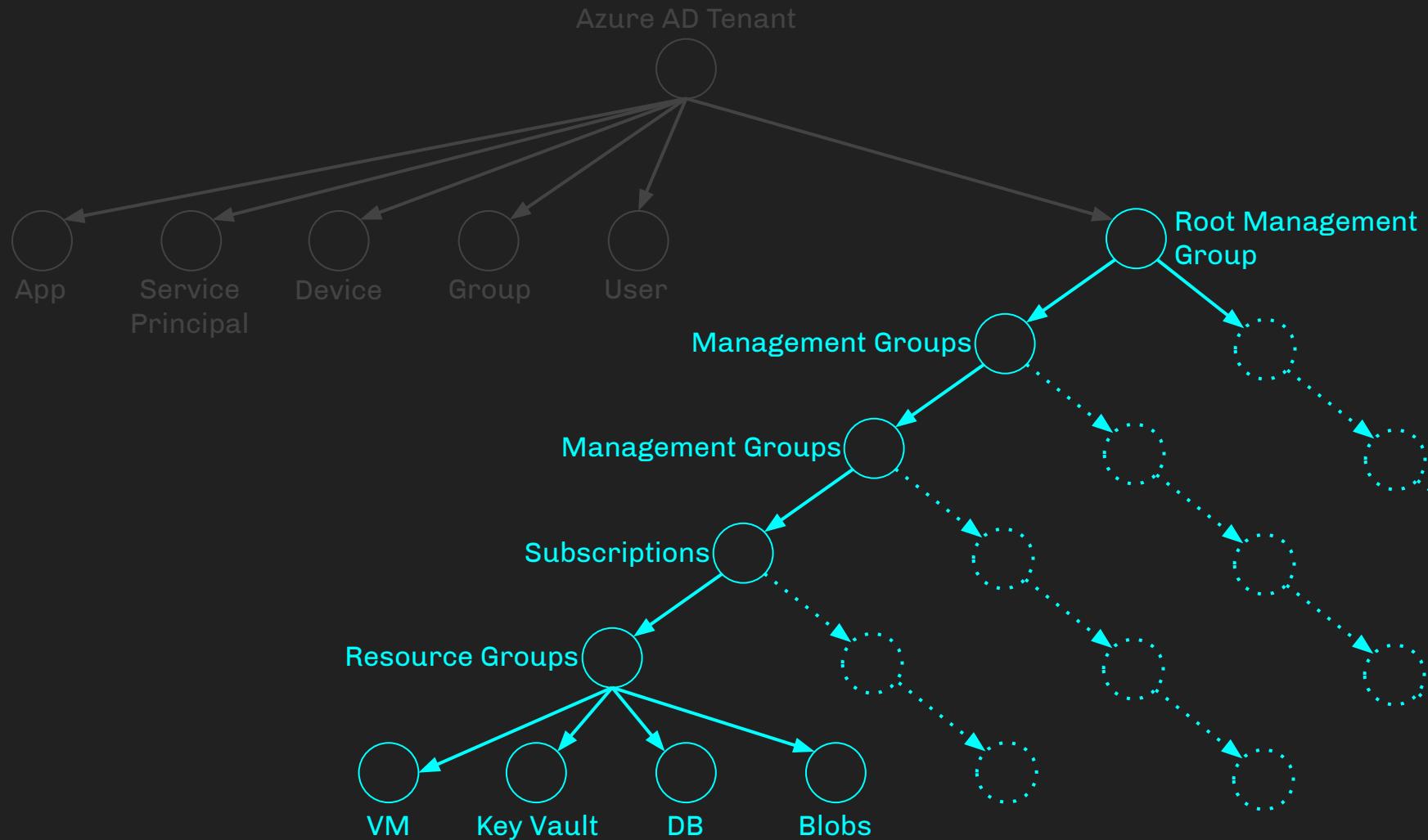
Access Control

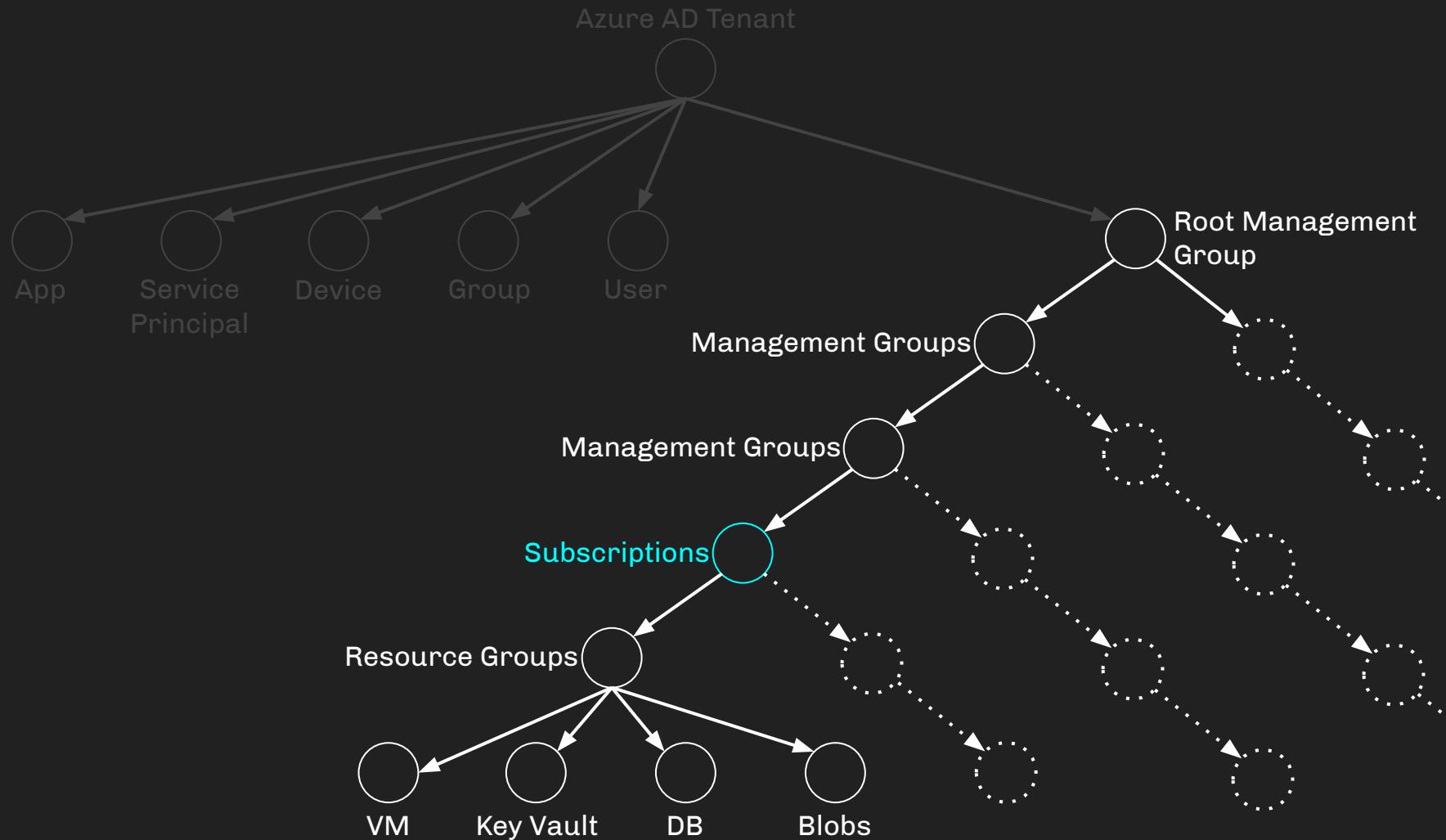


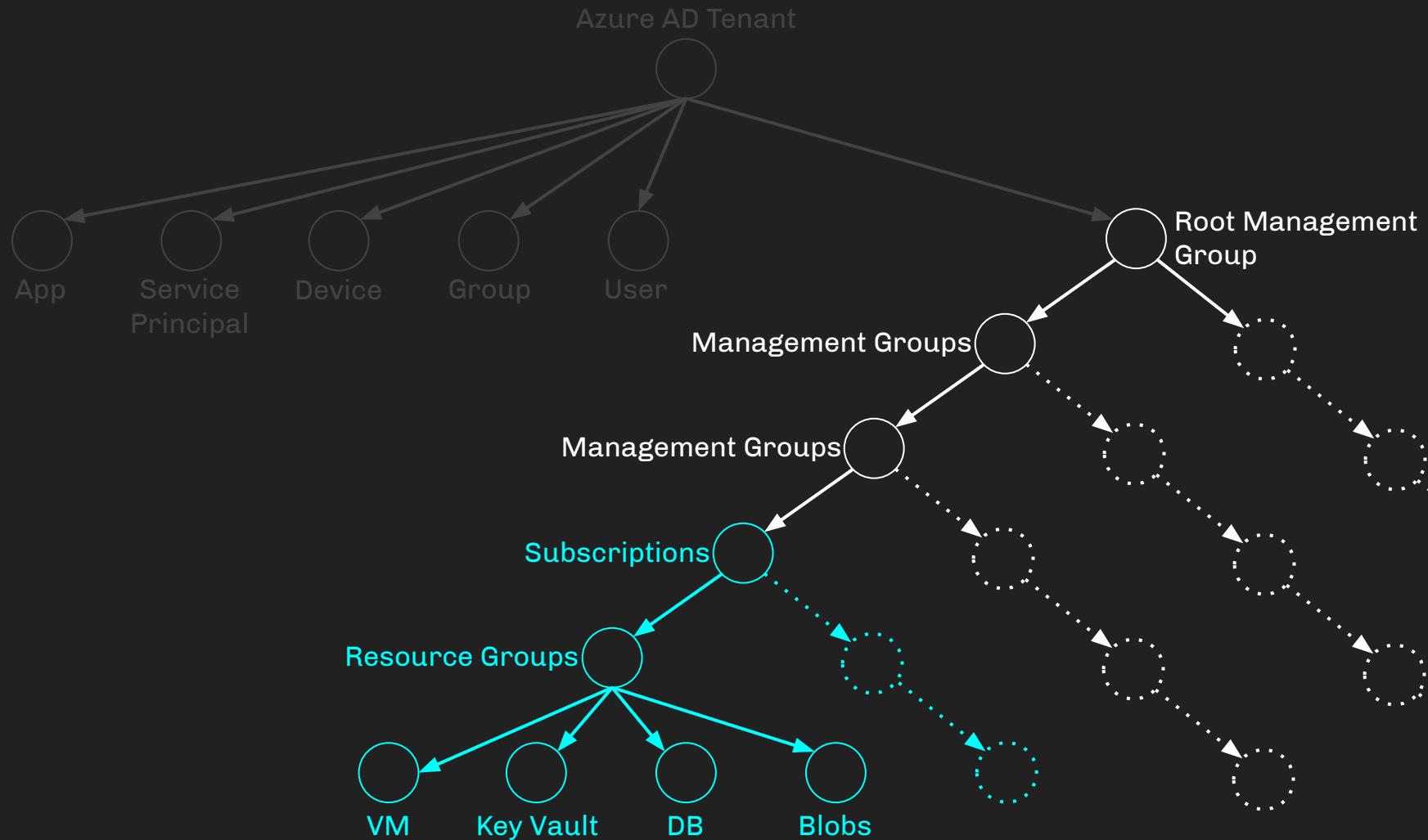


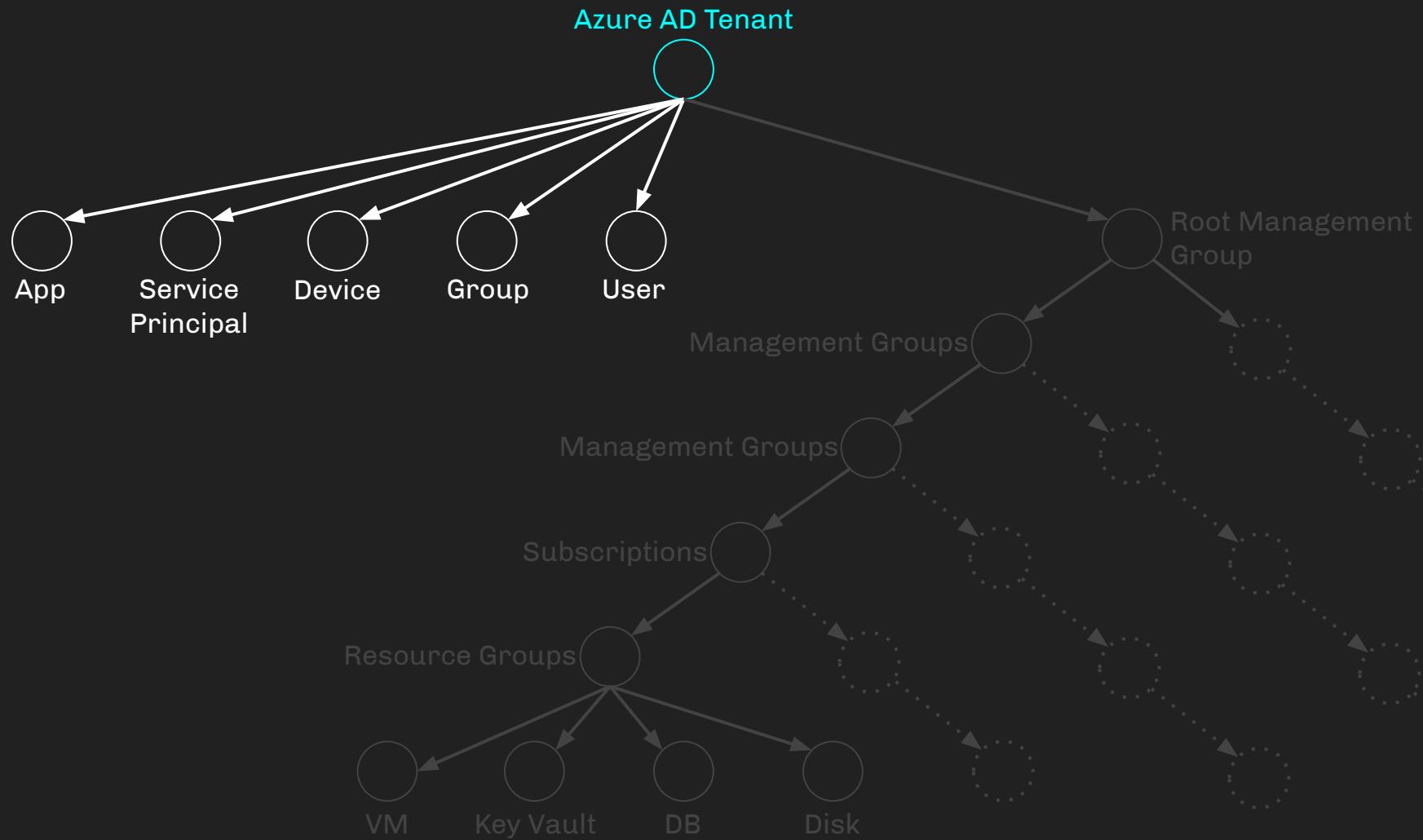


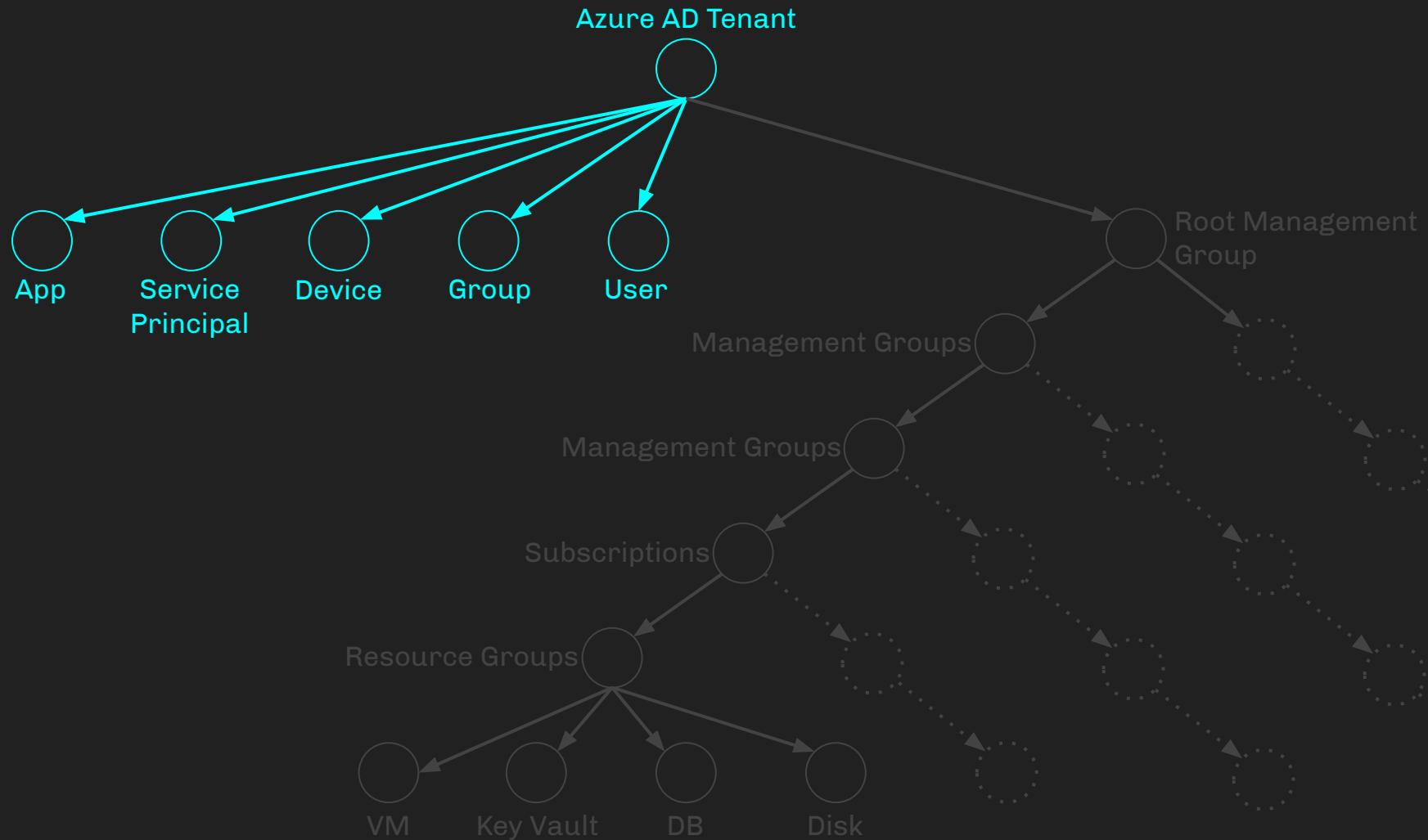


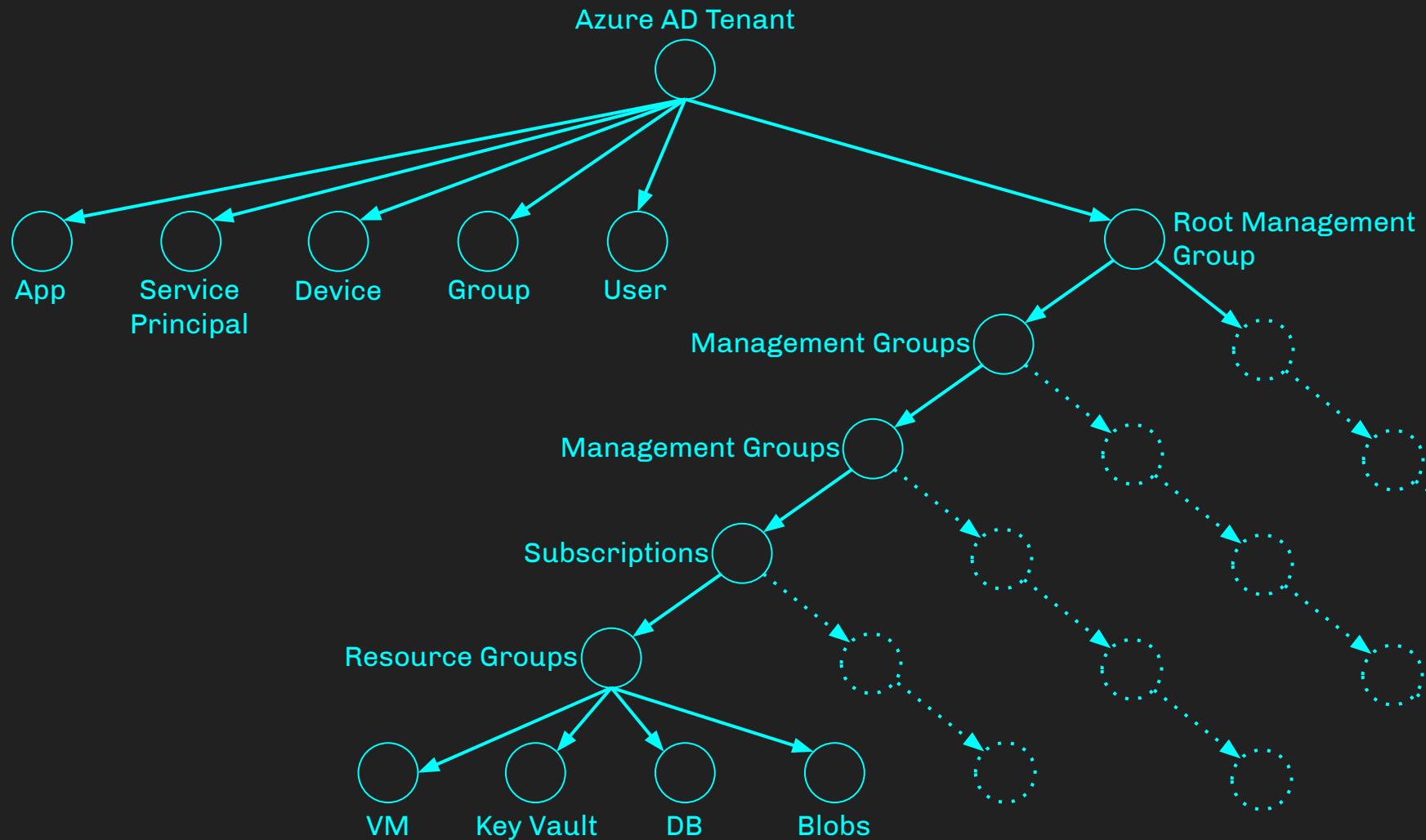












Agenda

Why Azure abuses?

Crash Course Through The Basics

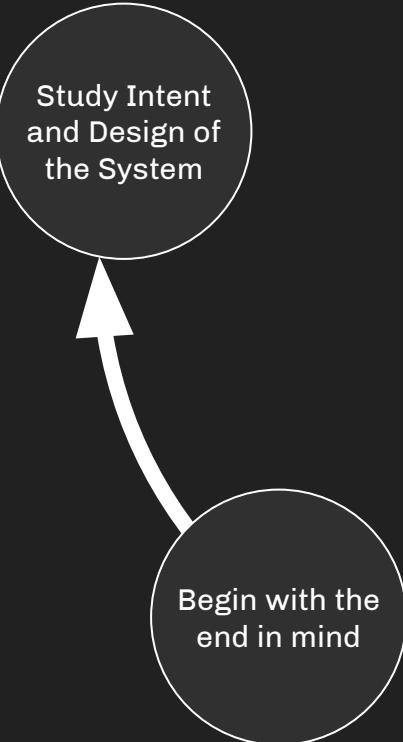
My Abuse Primitive Research Process: MS Graph Case Study

Where to find research ideas

Conclusion



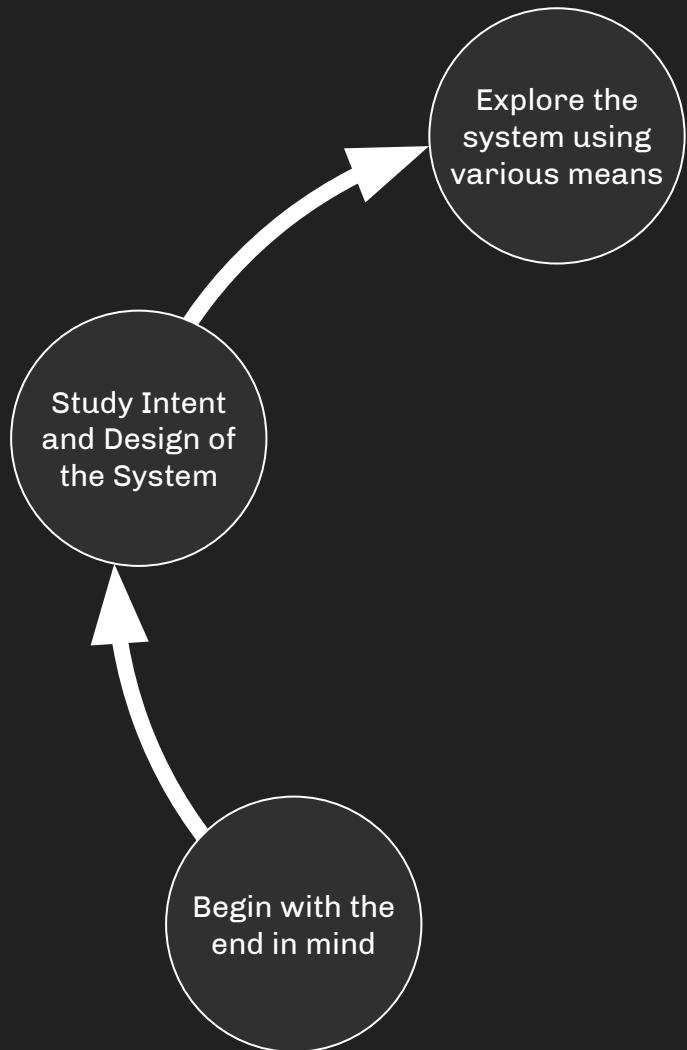
**Begin with the
end in mind**

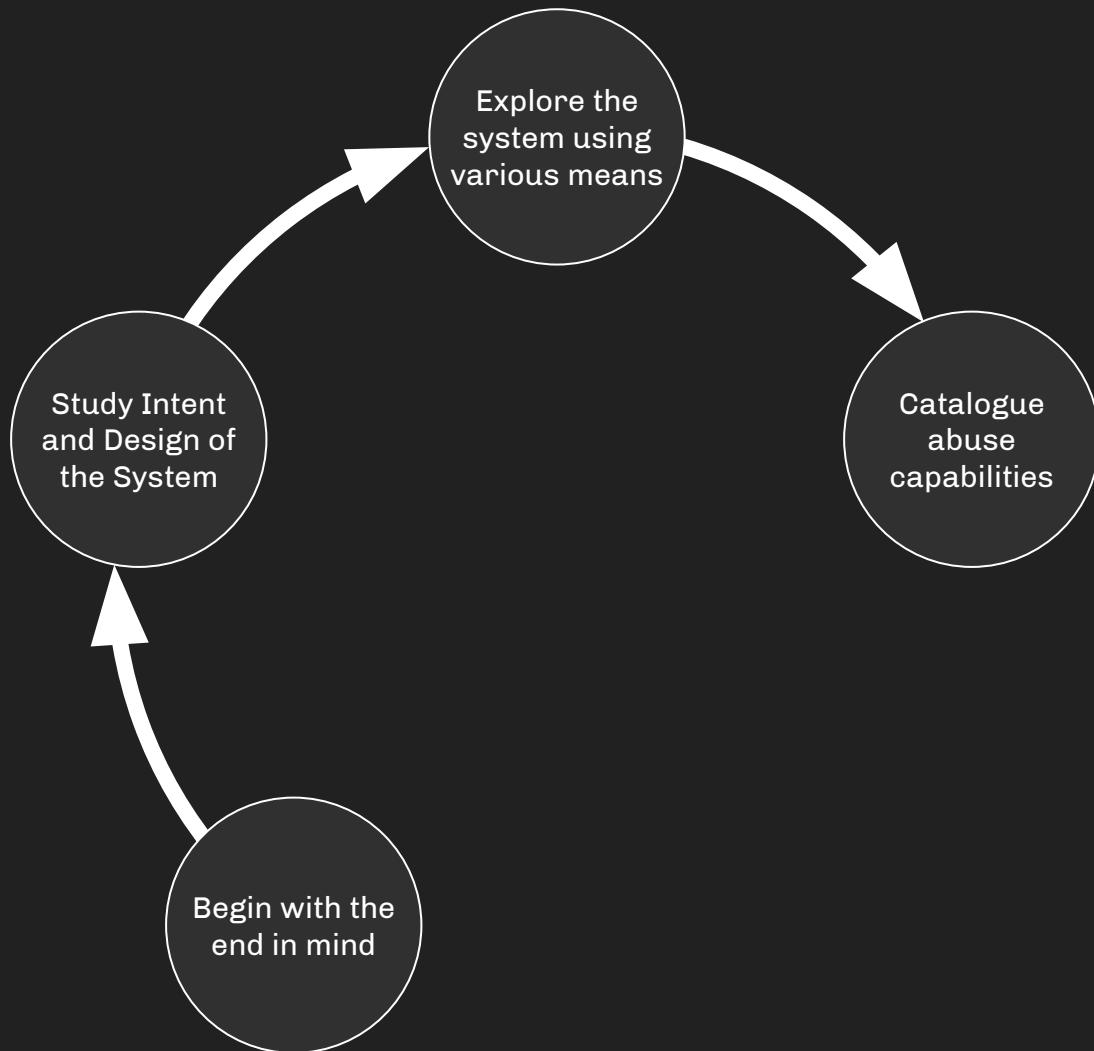


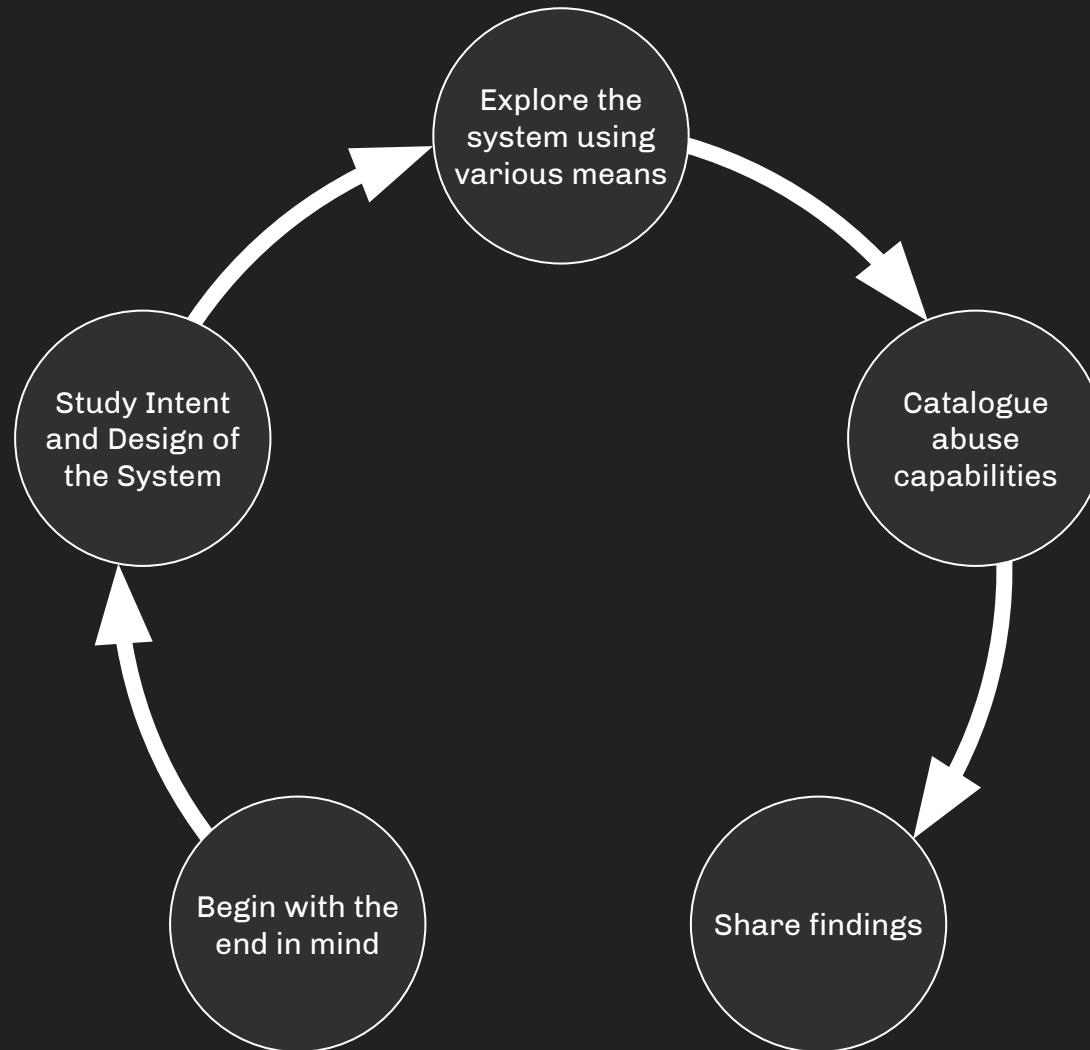
A diagram consisting of two white-outlined circles on a black background. A thick, white curved arrow points from the bottom circle up to the top circle. The top circle contains the text "Study Intent and Design of the System". The bottom circle contains the text "Begin with the end in mind".

Study Intent
and Design of
the System

Begin with the
end in mind







My Abuse Primitive Research Process



My Abuse Primitive Research Process





**Begin with the
end in mind**

I want to **understand**:

- The fundamental mechanics the system
- How the system interacts with other systems
- How the system can be abused



**Begin with the
end in mind**

I want to understand:

- The fundamental mechanics the system
- How the system interacts with other systems
- How the system can be abused

I want to **produce**:

- A blog/talk for others to understand and build on
- Example audit and abuse code
- Practical remediation guidance

Begin with the end in mind

I want to understand:

- The fundamental mechanics the system
- How the system interacts with other systems
- How the system can be abused

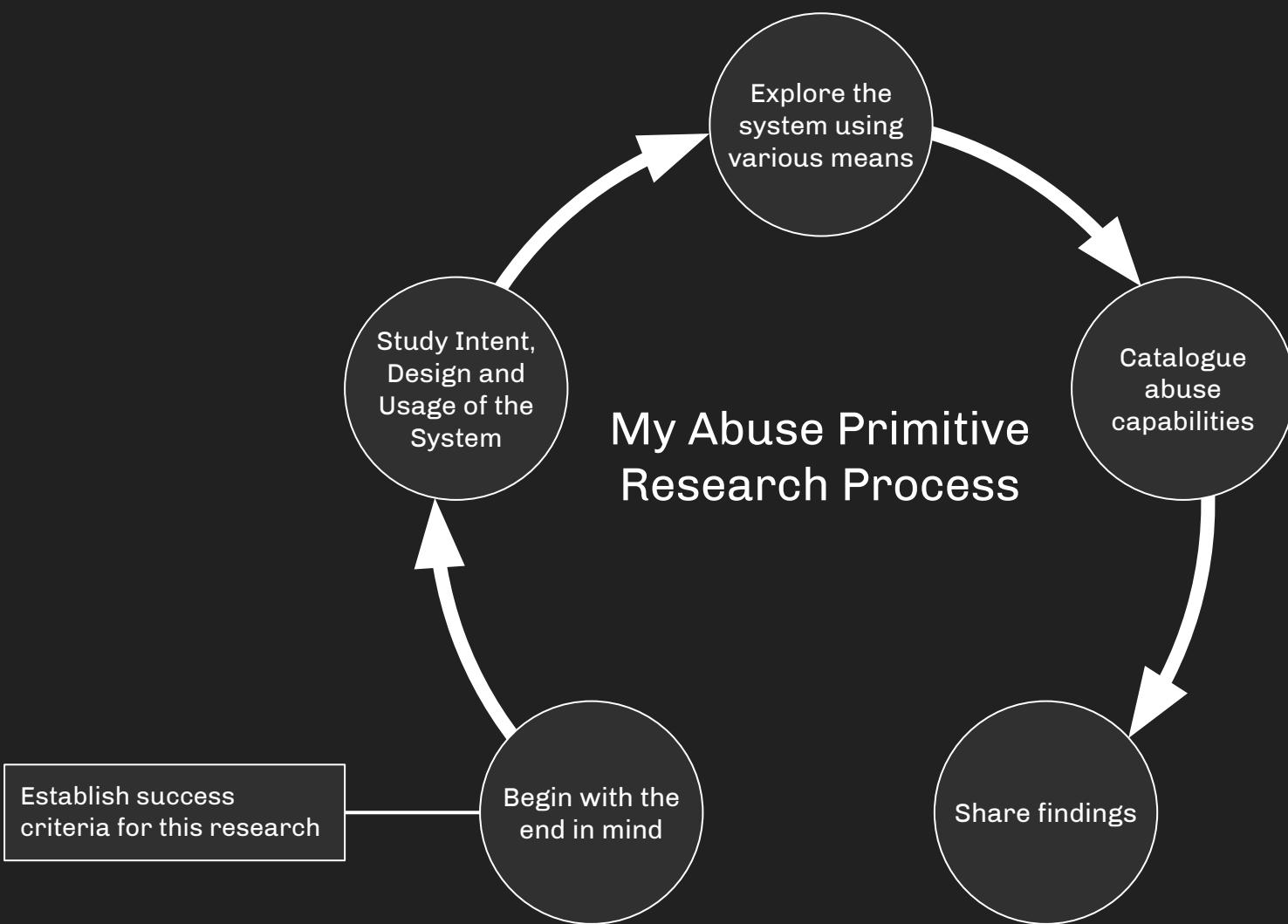
I want to produce:

- A blog/talk for others to understand and build on
- Example audit and abuse code
- Practical remediation guidance

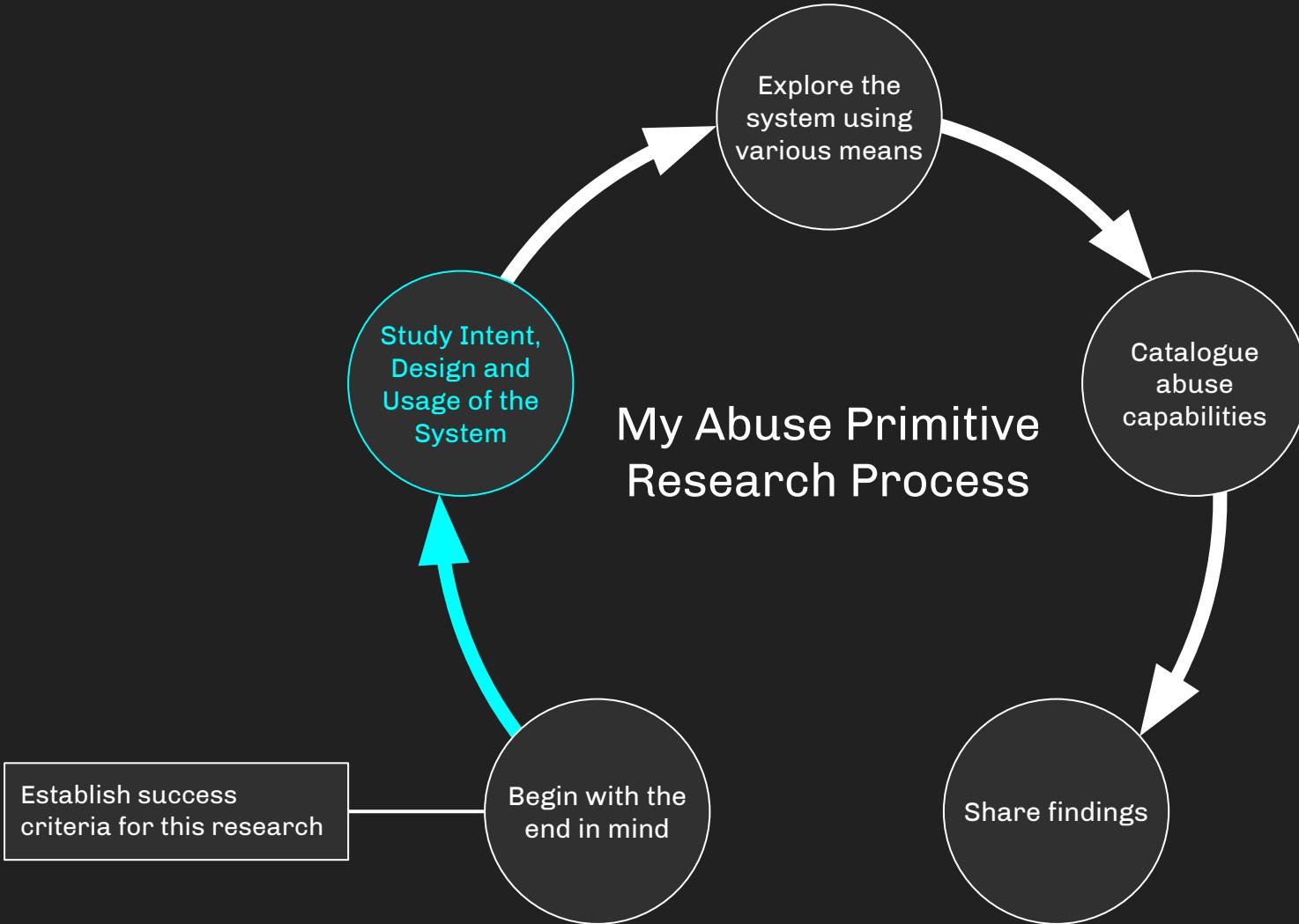
If appropriate for **BloodHound**, I want to **prepare for**:

- The impact on the existing graph model
- How to expand the graph model
- What data to collect and ingest, and how to get that data

My Abuse Primitive Research Process



My Abuse Primitive Research Process



**Study Intent,
Design and
Usage of the
System**

Official
Documentation

Technical

Non-Technical

Google



|



Google Search

I'm Feeling Lucky

Google



Microsoft MS graph



Google Search

I'm Feeling Lucky

[Filter by title](#)

Microsoft Graph documentation

Explore

[Overview of Microsoft Graph](#)

Services in Microsoft Graph

What's new

What's new highlights

API changelog

> Users you can reach

> Tutorials

Versioning and support

Terms of use

Learn

Users

> Groups

> Applications

> Accessing data at scale

> Calendar

> Cloud communications

Compliance

> Connecting external content

> Cross-device experiences

Customer booking (preview)

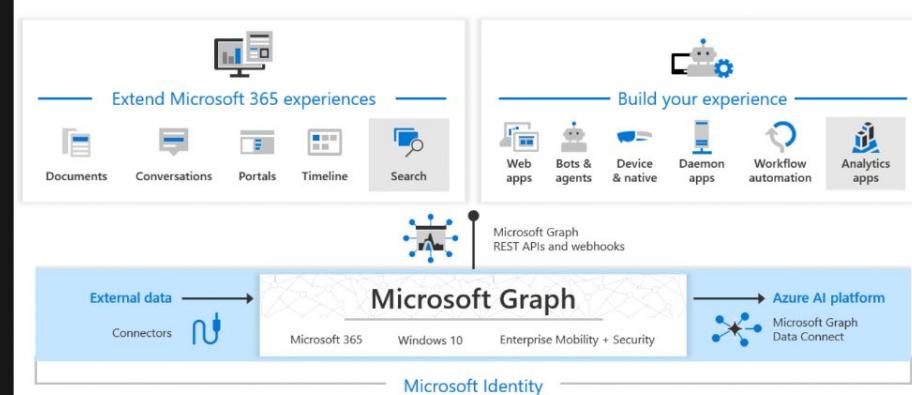
Overview of Microsoft Graph

Article • 11/11/2021 • 6 minutes to read • 16 contributors

[Like](#) [Edit](#)

Microsoft Graph is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that you can use to access the tremendous amount of data in Microsoft 365, Windows 10, and Enterprise Mobility + Security. Use the wealth of data in Microsoft Graph to build apps for organizations and consumers that interact with millions of users.

Microsoft 365 Platform



Data and services powering the Microsoft 365

In this article

[Data and services powering the Microsoft 365 platform](#)[What's in Microsoft Graph?](#)[What can you do with Microsoft Graph?](#)[Bring data from an external content source to Microsoft Graph](#)[Access Microsoft Graph data at scale using Microsoft Graph Data Connect](#)[When should I use Microsoft Graph API or Data Connect?](#)[Next steps](#)

 Filter by title

Microsoft Graph documentation

Explore

Overview of Microsoft Graph

Services in Microsoft Graph

What's new

What's new highlights

API changelog

> Users you can reach

> Tutorials

Versioning and support

Terms of use

Learn

Users

> Groups

> Applications

> Accessing data at scale

> Calendar

> Cloud communications

Compliance

> Connecting external content

> Cross-device experiences

Customer booking (preview)

Devices and apps

> Cloud printing

Corporate management

Cloud PC (preview)

What can you do with Microsoft Graph?



Use Microsoft Graph to build experiences around the user's unique context to help them be more productive.
Imagine an app that...

- Looks at your next meeting and helps you prepare for it by providing profile information for attendees, including their job titles and managers, as well as information about the latest documents they're working on, and people they're collaborating with.
- Scans your calendar, and suggests the best times for the next team meeting.
- Fetches the latest sales projection chart from an Excel file in your OneDrive and lets you update the forecast in real time, all from your phone.
- Subscribes to changes in your calendar, sends you an alert when you're spending too much time in meetings, and provides recommendations for the ones you can miss or delegate based on how relevant the attendees are to you.
- Helps you sort out personal and work information on your phone; for example, by categorizing pictures that should go to your personal OneDrive and business receipts that should go to your OneDrive for Business.
- Analyzes at-scale Microsoft 365 data so that decision makers can unlock valuable insights into time allocation and collaboration patterns that improve business productivity.

In this article

Data and services powering the Microsoft 365 platform

What's in Microsoft Graph?

| What can you do with Microsoft Graph?

Bring data from an external content source to Microsoft Graph

Access Microsoft Graph data at scale using Microsoft Graph Data Connect

When should I use Microsoft Graph API or Data Connect?

Next steps

Google

ms graph reset user password



Google Search

I'm Feeling Lucky

Version

Microsoft Graph REST API Beta

Filter by title

Get

Reset

Get operation status

> Certificate-based auth configuration

> Conditional Access

> Cross-tenant access (preview)

> Data policy operation

> Identity protection

> Identity provider

> Identity provider (deprecated)

> Invitation manager

> Organizational branding

> Policies

> Trust Framework Keyset

> Trust Framework policy

> User flows

> Governance

> Mail

> Notes

> Notifications (deprecated)

passwordAuthenticationMethod: resetPassword

Article • 11/29/2021 • 6 minutes to read • 8 contributors

Like

Edit

Namespace: microsoft.graph

Important

APIs under the `/beta` version in Microsoft Graph are subject to change. Use of these APIs in production applications is not supported. To determine whether an API is available in v1.0, use the `Version` selector.

Initiate a reset for the password associated with a `password authentication method` object. This can only be done by an administrator with appropriate permissions and cannot be performed on a user's own account.

This flow writes the new password to Azure Active Directory and pushes it to on-premises Active Directory if configured using password writeback. The admin can either provide a new password or have the system generate one. The user is prompted to change their password on their next sign in.

This reset is a long-running operation and will return a link in the `Location` header where the caller can periodically check for the status of the reset.

Permissions

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see [Permissions](#).

In this article

Permissions

HTTP request

Request headers

Request body

Response

Examples

Permissions

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see [Permissions](#).

In this article

- [Permissions](#)
- [HTTP request](#)
- [Request headers](#)
- [Request body](#)
- [Response](#)
- [Examples](#)

Permissions acting on self

The operation cannot be performed on a user's own account.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	Not supported.
Delegated (personal Microsoft account)	Not supported.
Application	Not supported.

Permissions acting on other users

Only an administrator with the appropriate permissions can perform this operation.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	UserAuthenticationMethod.ReadWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	Not supported.

For delegated scenarios where an admin is acting on another user, the admin needs one of the following Azure AD roles:

- Global administrator
- Privileged authentication administrator
- Authentication administrator

Google



ms graph permissions



Google Search

I'm Feeling Lucky

Filter by title

▼ Develop

▼ Get auth tokens

Overview

Basics

Register your app

Get access on behalf of a user

Get access without a user

Permissions

Manage app access (CSPs)

Limit mailbox access

Resolve authorization errors

> Use the API

> Migrate

> Use SDKs

> Use the Toolkit

▼ Resources

Best practices

Known issues

API changelog

Errors

v1.0 reference

Beta reference

Microsoft Graph permissions reference

Article • 02/17/2022 • 123 minutes to read • 103 contributors



For your app to access data in Microsoft Graph, the user or administrator must grant it the correct permissions via a consent process. This topic lists the permissions associated with each major set of Microsoft Graph APIs. It also provides guidance about how to use the permissions.

① Note

As a best practice, request the least privileged permissions that your app needs in order to access data and function correctly. Requesting permissions with more than the necessary privileges is poor security practice, which may cause users to refrain from consenting and affect your app's usage.

To learn more about how permissions work, see [Authentication and authorization basics](#), and watch the following video.



In this article

[Microsoft Graph permission names](#)[Microsoft accounts and work or school accounts](#)[Limits on requested permissions per app](#)[Permissions availability status](#)[User and group search limitations for guest users in organizations](#)[Limited information returned for inaccessible member objects](#)[Retrieving permission IDs](#)[Access reviews permissions](#)[Administrative units permissions](#)[Analytics resource permissions](#)[AppCatalog resource permissions](#)[Application resource permissions](#)[Audit log permissions](#)[BitLocker recovery key permissions](#)[Bookings permissions](#)[Calendars permissions](#)[Calls permissions](#)[Call records permissions](#)[Channel permissions](#)[Channel member permissions](#)[Channel message permissions](#)[Channel settings permissions](#)[Chat permissions](#)

Initial MS Graph Notes

- MS Graph is some kind of Azure-related service

Initial MS Graph Notes

- MS Graph is some kind of Azure-related service
- It exposes a REST API

Initial MS Graph Notes

- MS Graph is some kind of Azure-related service
- It exposes a REST API
- It can let you reset other users' passwords if you have the right permissions

Initial MS Graph Notes

- MS Graph is some kind of Azure-related service
- It exposes a REST API
- It can let you reset other users' passwords if you have the right permissions
- It seems to have a distinct permissions system versus Azure AD and Azure RM

**Study Intent,
Design and
Usage of the
System**

Official
Documentation

Technical
Non-Technical

Study Intent, Design and Usage of the System

People

Code
Repositories

Blogs

Talks

Official
Documentation

Technical

Non-Technical

Google



site:linkedin.com “Microsoft” “Graph” “Architect”



Google Search

I'm Feeling Lucky



site:linkedin.com "Microsoft" "Graph" "Architect"



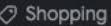
All



Images



News



Shopping



Videos



More

Tools

About 40,400 results (0.44 seconds)

<https://www.linkedin.com> › garethalunjones ... :

Gareth Jones - Principal API Architect for Microsoft Graph

Redmond, Washington, United States · Principal API Architect for Microsoft Graph · Microsoft

As the API **Architect** for the **Microsoft Graph**, I'm responsible for the all-up design choices and technical direction of Microsoft's most strategic API.

<https://ca.linkedin.com> › darrelmiller ... :

Darrel Miller - API Architect - Microsoft | LinkedIn

API Architect on Microsoft Graph ... As a member of the Microsoft Graph Developer Experience team, ... Senior Program Manager - Graph Developer Tooling.

<https://www.linkedin.com> › :

Joseph Cortese - Architect - Microsoft | LinkedIn

New Alexandria, Virginia, United States · Architect · Microsoft

Architect at Microsoft. Microsoft ... Senior Program Manager - Microsoft Graph at Microsoft ... Azure Architect, Principal Consultant at Microsoft.

<https://www.linkedin.com> › steveanonsen ... :

Steve Anonsen - Graduate Student - Biola University | LinkedIn

Fargo, North Dakota, United States · Graduate Student · Biola University

I'm API **Architect** for the **Microsoft Graph** (<http://aka.ms/graph>), driving API strategy, conventions and runtime for cloud APIs from Office and other ...



Darrel Miller

36.8K Tweets



Following

Darrel Miller

@darrel_miller

API Architect for Microsoft Graph. OpenAPI spec contributor. Co-chair IETF httpapi working group. Cloud Native Employee



Montreal, QC



Joined July 2010

3,353 Following **7,261** Followers



Followed by Matt Zorich, eliza, and 29 others you follow



Darrel Miller

36.8K Tweets

Following

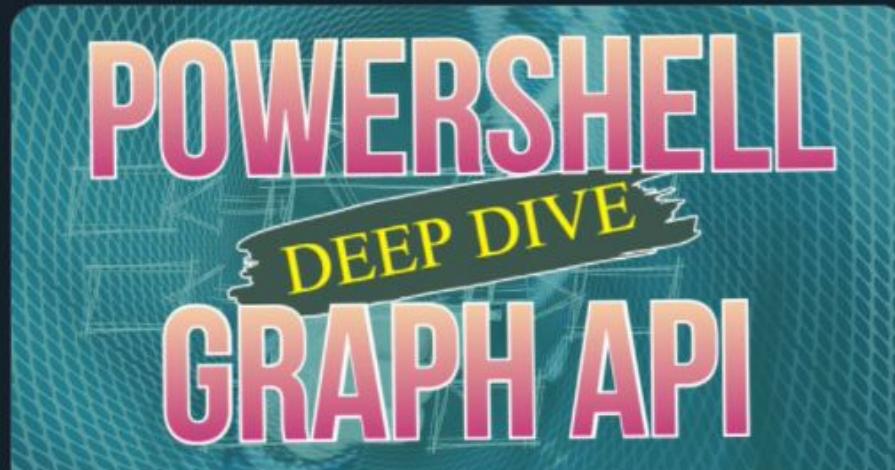
retweeted Darrel Miller Retweeted



Robert Dyas @robdyy · Jan 22

...

Detailed explanation about connecting to MS Graph via PowerShell:



thesysadminchannel.com

How To Connect To Microsoft Graph API Using PowerShell | Deep Dive

A deep dive to getting started with Microsoft Graph API. Learn how to connect using unattended automation or interactive sessions.



2



1



7



Announcing "30 Days of Microsoft Graph" Blog Series



Brian

October 30th, 2018

Throughout the month of November 2018, we are publishing daily articles (30 total) that aim to introduce developers to Microsoft Graph. We'll have content that covers 0-level to 200-level topics. Each post should take you 5-15 mins to read and try out the sample exercises. No prior knowledge of Microsoft Graph is required. We hope that beginners will quickly pick up the content and that experts will also learn a few new things.



Please be sure to bookmark this page (<https://aka.ms/30DaysMSGraph>) as the below list of topics will be updated as each day's post is published.

/YouTube

microsoft graph



Microsoft Graph

41K views • 2 years ago



Microsoft Graph exposes REST APIs and client libraries to access data on a number of Microsoft 365 services. In this episode ...

CC



Tips & Tricks

START CALLING THE GRAPH API IN UNDER 5 MINS!

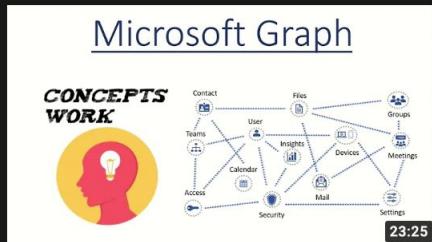
23:27

Start calling the Microsoft Graph API in under 5 minutes! | Tips & Tricks

25K views • 10 months ago



Learn tips & tricks to start calling the Microsoft Graph API in under 5 minutes. Microsoft Cloud Advocate, Dan Wahlin ...



What is Microsoft Graph?

16K views • 1 year ago



Microsoft #Graph #MicrosoftGraph What is Microsoft Graph? What is Microsoft Graph Api? What is Microsoft Graph Explorer?



What is Microsoft Graph?

24K views • 3 years ago



Learn about Microsoft Graph, an API that you can use to connect to various Office 365 services. It's a single endpoint that gets you ...

- ! [Search history](#)
- re [Recent activity](#)
- criptions [Descriptions](#)
-
- y [Your videos](#)
- y [Videos later](#)
- videos [Videos](#)
-
- ONS [Ones](#)
- |POOBear [POOBear](#)
- rousKing [rousKing](#)
- Jordan Alvar... [Jordan Alvar...](#)
- top Dan [top Dan](#)
- al [al](#)
- en the Bulldog [en the Bulldog](#)
- fromTOKYO [fromTOKYO](#)
- 18 more [18 more](#)
-
- YOUTUBE [YouTube](#)
- ibe Premium [ibe Premium](#)

Study Intent, Design and Usage of the System

People

Code
Repositories

Blogs

Talks

Official
Documentation

Technical

Non-Technical

Study Intent, Design and Usage of the System

People

Code
Repositories

Blogs

Talks

Official
Documentation

Technical

Non-Technical

Community

Chat & Forums

Repo Issues

(185 Open ✓ 505 Closed

Author ▾ Label ▾ Projects ▾ Milestones ▾ Assignee ▾ Sort ▾

● Powershell Microsoft.Graph- How to set MaxRetry ToTriage

#1106 opened 2 hours ago by MarkDordoy

● Continuous access evaluation error ToTriage

#1105 opened 5 hours ago by rickjansen-dev

● Users should use Authentication Providers to securely connect to Microsoft Graph ToTriage

#1104 opened yesterday by sebastienlevert

● Authentication Providers ToTriage

#1103 opened yesterday by sebastienlevert

● Set-MgApplicationLogo requires Content-Type to be image/* ToTriage

#1097 opened 4 days ago by peombwa

● Clean-up AzDo Pipeline for Continuous Release

1



#1096 opened 4 days ago by peombwa

● Selecting fields with Get-MgSiteListItem ToTriage

#1094 opened 5 days ago by lkubat

● Invoke-MgInvalidateUserRefreshToken throwing exception, although operation succeeds ToTriage

#1092 opened 7 days ago by khant414

● get-mguser doesn't always return Id ToTriage

#1091 opened 7 days ago by anwarmahmood1

● Searching for equivalent command ToTriage

#1090 opened 7 days ago by Tiberriver256

● Issue adding an application to Catalog through PowerShell SDK - New-MgEntitlementManagementAccessPackageResourceRequest ToTriage

#1089 opened 7 days ago by purish87

● Create documentation for the cmdlets Authentication module Request: Documentation

#1088 opened 8 days ago by maisarissi ↗ 03/22



3

● That's it! Now Microsoft Graph PowerShell module is ready to use!

1

Initial MS Graph Notes

- MS Graph is some kind of Azure-related service
- It exposes a REST API
- It can let you reset other users' passwords if you have the right permissions
- It seems to have a distinct permissions system versus Azure AD and Azure RM

Updated MS Graph Notes

- Microsoft is investing into MS Graph as a sort of “API for APIs”, a unifying endpoint that may eventually allow for indirectly interacting with any object in any service just by interfacing with MS Graph.

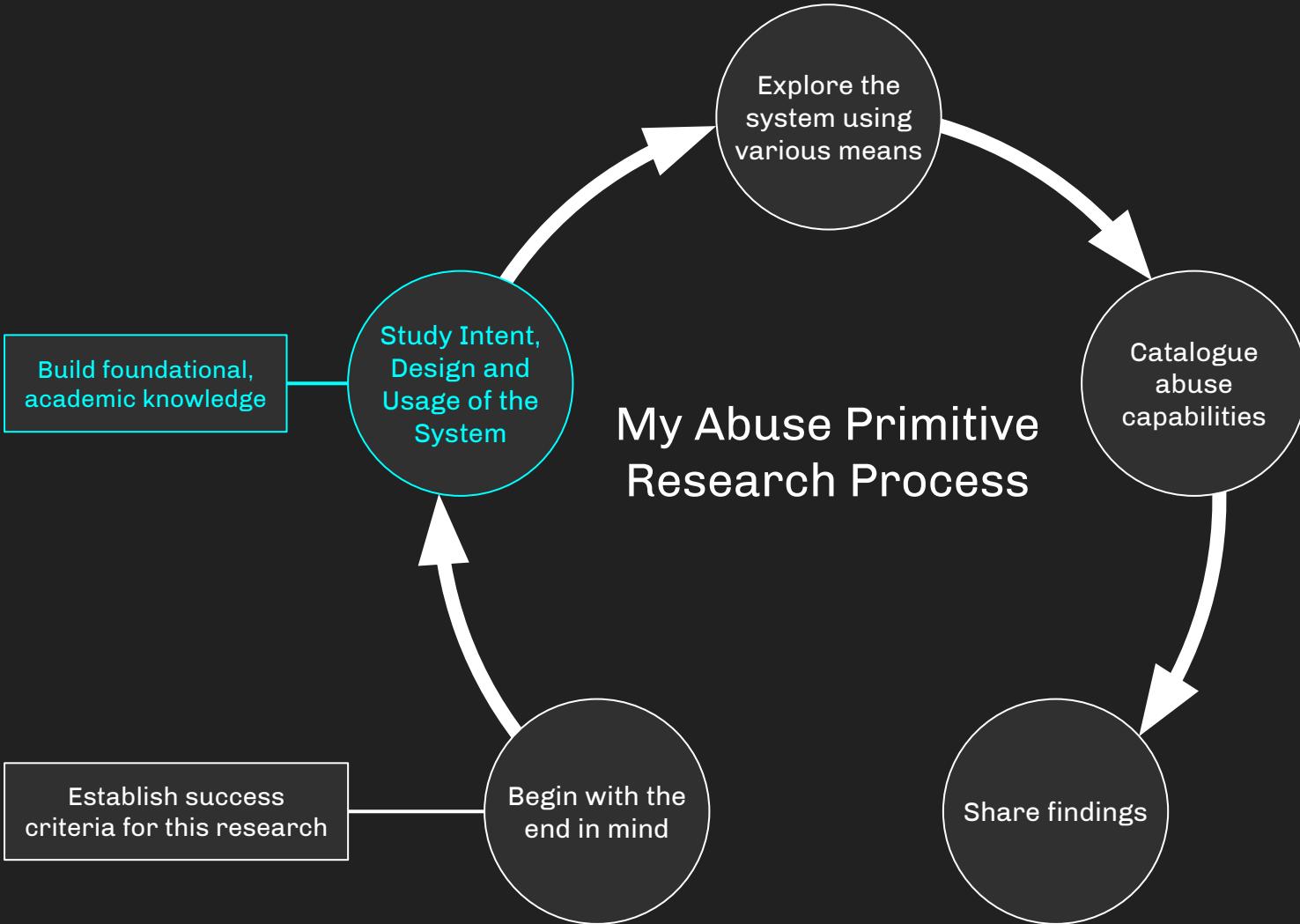
Updated MS Graph Notes

- Microsoft is investing into MS Graph as a sort of “API for APIs”, a unifying endpoint that may eventually allow for indirectly interacting with any object in any service just by interfacing with MS Graph.
- MS Graph’s REST API is instantiated into every Azure tenant as a Resource App (aka Enterprise App, aka Service Principal, aka First Party App).

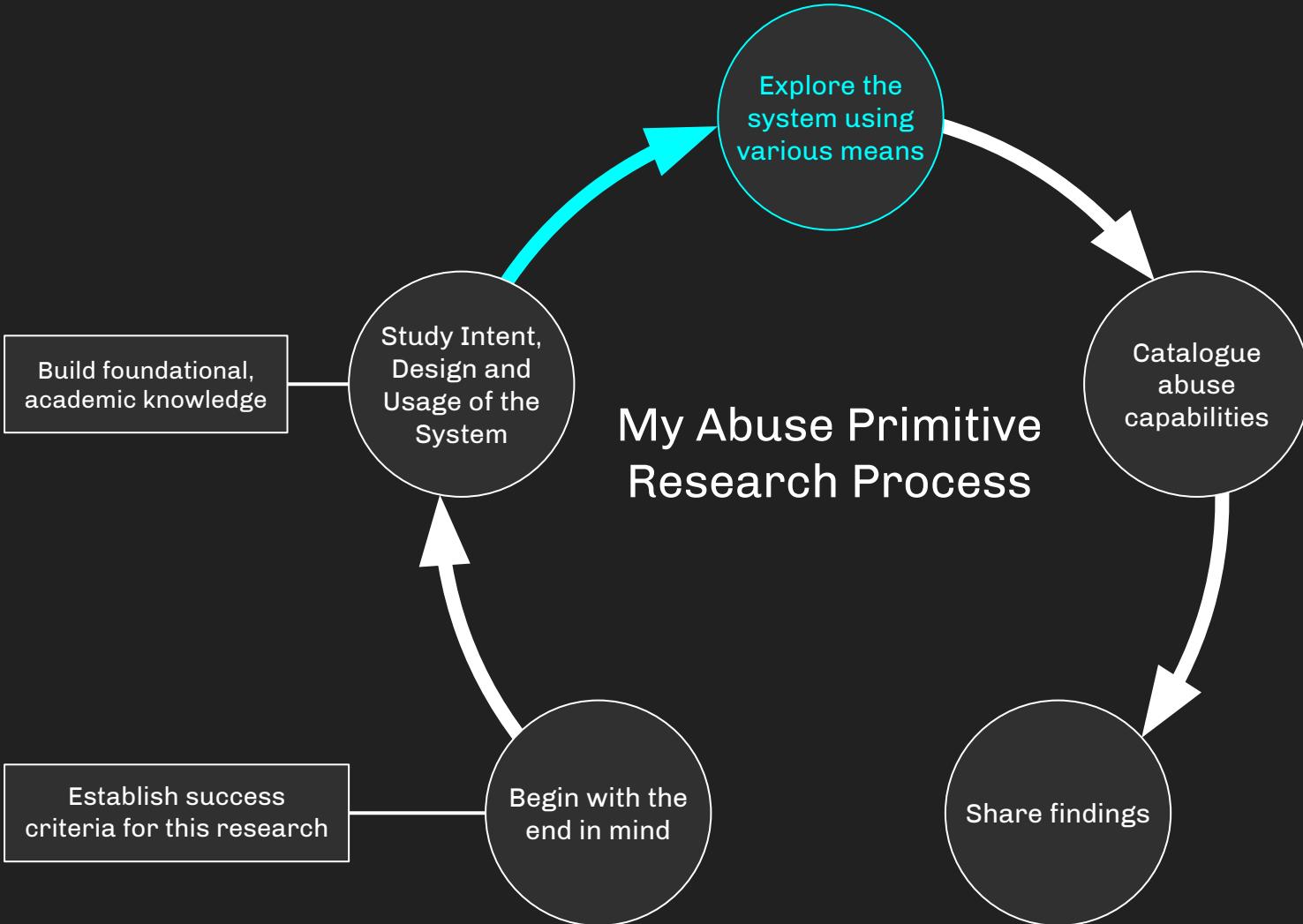
Updated MS Graph Notes

- Microsoft is investing into MS Graph as a sort of “API for APIs”, a unifying endpoint that may eventually allow for indirectly interacting with any object in any service just by interfacing with MS Graph.
- MS Graph’s REST API is instantiated into every Azure tenant as a Resource App (aka Enterprise App, aka Service Principal, aka First Party App).
- MS Graph brokers requests to particular Azure services, including privileged action requests like resetting passwords or adding users to security groups.

My Abuse Primitive Research Process



My Abuse Primitive Research Process



You must go beyond the documentation.

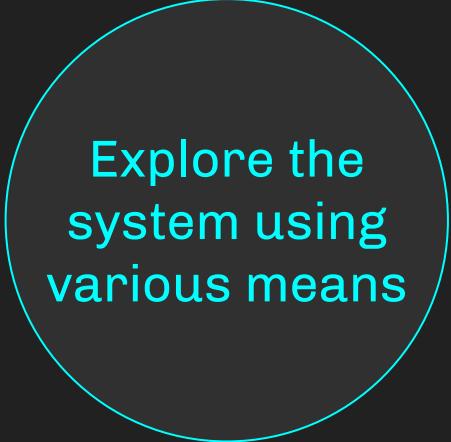
- These systems are **interconnected** in undocumented and non-public ways

You must go beyond the documentation.

- These systems are interconnected in undocumented and non-public ways
- Documentation often doesn't keep up with changes

You must go beyond the documentation.

- These systems are interconnected in undocumented and non-public ways
- Documentation often doesn't keep up with changes
- Tooling based only on documentation is almost always **inaccurate, unreliable** tooling.



Explore the
system using
various means

Explore the
system using
various means



Azure Portal GUI

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > SpecterOps Development > Users > Andy Robbins

Andy Robbins | Profile

User

Diagnose and solve problems

Manage

Profile

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Creation time
11/1/2021, 9:59:21 AM

Last sign-in date
3/16/2022, 10:32:42 AM

User Sign-ins

Group memberships

AR

Name: Andy Robbins

First name: Andy

Last name: Robbins

Identity

Network

Performance

Memory

Application

Security

Lighthouse

Reorder

Preserve log

Disable cache

No throttling

Filter

Request URL: https://graph.microsoft.com/v1.0/users/16571a9f-a0b4-476a-87e8-14dca511b9a3?\$select=displayName

Request Method: GET

Status Code: 200 OK

Remote Address: 20.190.151.37:443

20 requests | 80.4 kB transferred | 110 kB resources

 Andy Robbins | Profile
User

 Edit  Reset password  Revoke sessions  Delete  Refresh |  Got feedback?

Andy Robbins

a Robbins@specterdev.onmicrosoft.com



Creation time
11/1/2021, 9:59:21 AM



Last sign-in date
3/16/2022, 10:32:42 AM

Identity

Name
Andy Robbins

First name
Andy

Last name
Robbins

The screenshot shows the Chrome DevTools Network tab. A context menu is open over a network request, with the 'Copy as PowerShell' option highlighted by a red arrow. The menu also includes options like 'Copy link address', 'Copy response', 'Copy stack trace', 'Copy', 'Block request URL', 'Block request domain', 'Replay XHR', 'Sort By', 'Header Options', and 'Copy all as'. The main network table displays various requests with columns for initiator, timing, and response details.

```
1 $session = New-Object Microsoft.PowerShell.Commands.WebRequestSession
2 $session.UserAgent = "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36"
3 Invoke-WebRequest -UseBasicParsing -Uri "https://graph.microsoft.com/v1.0/users/16571a9f-a0b4-476a-87e8-14dca511b9a3?`$select=displayName`"
4 -WebSession $session
5 -Headers @{
6 "x-ms-client-session-id"="f9bdae195136432c82b5f27fdddf1ad2"
7 "DNT"="1"
8 "x-ms-command-name"="UserManagement%20-%20UserAllPropertiesDataMsGraph"
9 "Accept-Language"="en"
10 "Authorization"="Bearer eyJ0eXAiOiJKV1QiLCJhbGwiOiJzZXI6Iklk3WHa3cy14MHV6RWJVa1VRb0NWZ1JiSEdXbU9G0W9zUllwbUltek53REKiLCJhGci0iJSUz1NiIsIng1dCI6ImpTMVhvMU9XRgpfNTJ2YndHTmd2U08yVnpNYiSImtpZCI6ImpTMVhvMU9XRgpfNTJ2YndHTmd2U08yVnpNYyJ9eyJhdWQiOjodHRwczovL2dyYXB0Lm1pY3Jvc29mdC5jb20vIiwiXNzIjoiaHR0cHM6Ly9zdHMu2luZG93cy5uZXQvNmMxMmIwYjAtYjJy00YTczLTgyNTItMGI5NGJmY2EyMTQ1LyIsImlhcdI6MTY0NZU1Mj04NSwibmJmIjoxNjQ3NTUyNTg1LCJleHAi0jE2NDc1NTc4MDIsImFjY3Qi0jAsImFjciI6IjEiLCJhaw8i0iJFmlpWulqYWZXumx1lKytaaj1lVHRTVFdybGY3d2VTWjFLQ3p0L1JVL1BhR200SU96bXNCiawiY1YjpBInB3ZCJdlCJhcHBfZGlcGxheW5hbWUi0iJBREliaXphVVgiLCJhcHBpZCI6IjcoNju4MTM2LTE0ZMmtNDYzMC1hZDl1LT1ZTE2MGZmMGZjNiIsImFwCGlkYWhNyIjoiMiIsImVbnRyb2xZIpbImNhX2VuZijdLCjmyW1pbHlfbmFtZSI6IlJvYmJpbmMiLCJnaXZlbl9uYW1lIjoiQW5keSiIsImlkdkHlwIjoiXnlciIsImlkWRCkiI6IjIwOC43MS4xNjQuMTk1IiwibmFtZSI6IkFuZHkgUm9iYmlucyIsIm9pZCI6IjE2NTcxYTlmLWEwYjQtNDc2YS04N2U4LTE0ZGnhNTExYjIhMyIsInBsYXRmIjoiNSIsInB1aWQo0iIxMDAzmJAwMUEwQThFQzREIiwigmgioIiwlkFWRUFzTEFTYk15ewMwcunVZ3VvdjhvaFJRTUFBUFBQUFBFQxdBQUFBUFCUKfLYy4iLCjzY3Ai0iJBY2Nlc3NSZXZpZXcuUmVhZFdyaxXRLlkFsbCBbdWRpdExvZy5SZWFkLkFsbCBEaXJLY3RvcnkuQWnjZXNzQXNVc2VylkFsbCBEaXJLY3RvcnkuUmVhZC5BbgwgRGLyZWN0b3J5LljYWrxcm10ZS5BbgwgRGLyZWN0b3J5UmVjb21tZW5kYXRpb25ZLlJlyWQuQwsIGVtYwlsIEVudG10bGVtZW50TWFuYwdlbwVudC5SZWFkLkFsbCBHcm91cC5SZWFkV3JpdGUuQwsIElkZw50aXR5UHJvdmlkZXIUUmVhZFdyaxRRLkFsbCBJZGVudGL0eVJpc2tFdMVudC5SZWFkV3JpdGUuQwsIElkZw50aXR5VNlckZsb3cuUmVhZC5BbGwgb3BlbmkIFBvbGljeS5SZWFkLkFsbCBQb2xpY3kuUmVhZFdyaxRRLkF1dGh1bnRpY2F0aW9uRmxvd3MgUG9saWNLljYWrxcm10ZS5BdXRoZw50awNhdlGlvbk1ldGhvZCBQb2xpY3kuUmVhZFdyaxRRLkNvbmrpdGvbmfswQWnjZXNzIHByb2ZpbGUGUmVwb3J0cy5SZWFkLkFsbCBSb2x1TWfuYwdlbwVudC5SZWFkv3JpdGUuRGLyZWN0b3J5IFNlY3VyaXR5RXZlbnRzLlJlyWrxcm10ZS5BbgwgVHJ1c3RGcmFtZDvcmtLZxltZxQuUmVhZC5BbgwgVXNlcis5FeHBvcnQuQwsISFVzZXIUUmVhZFdyaxRRLkFsbCBvc2VyQXV0aGVudGljYXRpb25NZXRob2QuUmVhZFdyaxRRLkFsbCIsInN1YiI6InhidUhwTHRfbVRHRURPcldXOFJUMUhBdW5pWi0xbDV2S0h5cEtUT3gzMFUiLCJ0ZW5hbnRfcvmnaw9uX3Njb3BLiijo1TkEiLCJ0aWQo0iI2YzEyYjBiMC1iMmNjLTRhNzMt0DI1Mi0wYjk0YmZjYTIXNDUiLCJ1bm1xdWfbmftZSI6ImFyb2JiaW5zQHnwZwN0ZXjkZXYub25taWNyb3NvZnQuY29tIiwidXBuIjoiYXJvYmJpbnaC3B1Y3RlcmlRldi5vbm1pY3Jvc29mdC5jb20iLCJ1dGki0iI3Q3lGbTZ5R0xvn1kxNzRKaTdZUUFBiwiidVmVjyjoiMS4wIiwid2lkcyI6Wyl2MmU5MDM5NC020WY1LTQyMzct0TE5MC0wMTIxNzcxNDVlMTAiLCJiNzlmY0ZC0zZwY5LTQ2Dkt0DE0My03NmIx0TRl0DU1MDkiXSwieG1zX3N0Ijp7InN1YiI6IldfaGRJWDlmRjR5S1pRRVRy0HN6N21YMFZzeDBnSVg0Wkl2Q3FDRxpmTFUifSwieG1zX3RjZHQi0jE10Dg2MDI4NzN9.ahiEMnLxJusjxBa4VAFJJE64hkI7bpAFJJ0XMQ5WzRprLck2BbjvPIbUat2n0LJl4ZagsqVW-mojxdcCtmemoMIKYWPebYnK9hwnFHLSmkAYSGPyuSkYPDGcxHAHeYV0oiKQoAPL58lgv4pi32YkAjXdccnqv0amKaLMA089kUcv13tZqY0yPaAIN0iM0--5og78M0BV8RYQHP3WinvT6Jg8P7NxDpgiUK22kHvlJxj-D_EMMsLEC20Ey7ImwESpNb1vkrGHCu4IhUKN6ljoSkytlvxJ6JCtK7gksqCwbtDr81e5fohn5SI5mRnhsxq-WE8ZT8wrrtrTNArFlkQ00g"
11 "x-ms-effective-locale"="en.en-us"
12 "Accept"="*/*"
13 "Referer"=""
14 "x-ms-client-request-id"="b0864d22-023e-4e77-afcf-9b36de5c7059"
15 }
```

```

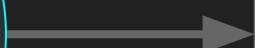
PS /Users/andyrobbins> $session = New-Object Microsoft.PowerShell.Commands.WebRequestSession
PS /Users/andyrobbins> $session.UserAgent = "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36"
PS /Users/andyrobbins> Invoke-WebRequest -UseBasicParsing -Uri "https://graph.microsoft.com/v1.0/users/16571a9f-a0b4-476a-87e8-14dca511b9a3?`$select=displayName"
>> -WebSession $session
>> -Headers @{
>> "x-ms-client-session-id"="f9bdae195136432c82b5f27fdddf1ad2"
>> "DNT"="1"
>> "x-ms-command-name"="UserManagement%20-%20UserAllPropertiesDataMsGraph"
>> "Accept-Language"="en"
>> "Authorization"="Bearer eyJ0eXAiOiJKV1QiLCJub25jZSI6IkI3WHA3cyI4MHV6RWJVa1Rb0NWZTJiSedXbU90WPzUllwbuUtek53REk1CJhbGciOjISUzI1NisInq1dCi6ImpTMvhM
U9XRGpfNT2YndHTmd2UUmxVnpNYyIsImtpZCI6ImpTMVhvMu9XRGpfNTJ2YndHTmd2U8yVnpNYyJ9.eJhdWQioiOjhdHRwczovL2dyYXBoLmipY3Jvc29mdC5jb20vIiwinXnZijoiaHR0cHM6Ly9zdH
Mud2luZG93cy6UxQvNmMiwjAtYjIyy00YTczLtgynTqIyisIm1hdC16MTY0NzU1mjU4NsWibmJmIjoxNjQ3NTUyNTg1LCJleHaiOjE2NDc1NTc4MDisImFjy3Q1ojsAsImfj
ciI1jIjEiLCJhaW8iOjFmlpnWUljQWxUmx1Kytaaj1lVHVRTFdybGY3d2VTwjFLQ3p0L1JVL1BhR200SU96bXNCiwiWY1yIjpBnB3ZCJdLCJhcHBFZGlcGxheW5hbWUioiJBREliaXphVVgilCJhcH
BpZC16ijc0nJu4MTM2TE02MtNDYzMc1hZD1LT12ZTE2WZMzMgZJNiisImFcwMnbnRyb2xZjpbImNhX2vUzJjdLCJmYW1pH1fbmfztS1611jvYmJpbnMilCJnaXZlbWY11
IjoiQW5keIsIm1kdHlwIjoiDxN1ciIsIm1wYRkcI6ijIwOC43MSAxNjQmtK11iwiwmFtZSI6IkFuZKhgUm9iYmlucyIsIm9pZC16ijE2NTTxYTlmLWEwYjqtNdc2YS04N2u4LTE0ZGNhNTEyJ1hMy
IsInBsYXRmIjoiNSisInB1aQioiIxMDAzmjAwMuewQThFQzREIiwigmoiIwlkFwRUFzTEFTYK15ewMwcUNVZ3VVdjhvaFJRTUFBFQUBQxFQUBQxFQUCFKFLy4iLCJzY3A1oiJBY2N1c3NS
ZXZpZxcuUmVhZFdyaXRlkFsbCBBdWRPdExvZy5SZWFkLkFsbcBeaXJ1y3RvcnkuQWnjZXNzQXNvc2VylFsfbcBeaXJ1y3RvcnkuUmVhZC5BbGwgRGlzZWN0b3J5l1J1yWRXcm1oZSSBbGwgRGlzZWN0b3
J5UmVjb21tZW5kYXRpb25zL1YwQWxsIEvUdG1obGvtWfUdWlbvUdCSZWfkLkFsbCBHcm91cc5SZWfkV3JpdGUuQWxsIE1k1Zw50aXR5UHJvdmlkZXIUUmVhZFdyaXR1LkFsbCBJ
ZGVvudG10evJpc2tFdmVudCSZSWfkV3jpdGUuQWxsIE1kZw50aXR5vXN1ckZsb3cuUmVhZC5BbGwgB381bmlkIFBvbGlje55SZWFkLkFsbcBQb2xpY3kuUmVhZFdyaXR1LkF1dGhbnRpY2f0awu9uRmxv3d
MgUG9saWN5L1J1yWXRxm10Zs5BdXrRoZw50aWhdGlvbk1ldGhvZCQBk2pxY3kuUmVhZFdyaXR1LkNvbRpdGlvbmFsQWnjZXNzIHByb2ZpbGUGUmVwb3J0cy5SZWFkLkFsbCBSb2x1TwFbYwdbWvudC5S
ZWFkv3JpdGUuRgljZwnB3J5F1Ny3YxaKR5RxlbnRzllJ1yWRxm1oZs5BbGwgVHj1c3RgcmtLZxvcm1LZx1TzQuUmVhZC5BbGwgVXN1ci5fehBvcmQuQWxsIFVzZxiuUmVhZFdyaXR1LkFsbCBv2
VyxQV0aGVduG1jYRxpB2NzXZRob2QuUmVhZFdyaXR1LkFsbCisInN1YiI6InhidUhWthrbVRHRUPcldFJUMuhBdWsp0xbDV2S0h5ceTUT3gzMFUj1LCj0Zw5hbnfcVmaw9uX3NjB3B1IjoiTkEi
LC00awQioiI2yEyjBimC1iMnjLTRhnzMtODi1Mi0wyjk0YmzYiTtndU1LCj1bmlxdWVfbmFtzS16imFyb23iaW5zQHnwzWNBZJXKZXYub25taWnyb3nVzNquY29tliwidXbuIjoiYXJvYmJpbnNaC3
B1y3RlcmRldi5vbm1pY3Jvc29mdC5jb201LCj1dGki0i13Q31GbTZ5R0xvn1kxzRkaDzZuUFBLiwidmVyljoiMs4wiwid21kcyI6wyI2Mmu5MDMSNC020WY1LTQyMzctOTE5MC0wMTIxNzcxNDVlMTAi
LCJinZmlmY0ZC020DktODE03NMixOtr10DU1XswieG1zXN0iJp7In1Yi6I1ldfaGRJWDlrmRjR5SlpRRVRYOHN621YMFZzeDBnSVg0Wkl2Q3FDRxpmTFUifswieG1zX3RjZHQi0j
E10Dg2MDIAzN9.ahiEmnLxusjxBa4VaFJE64hk17bpAFJ0XMQ5WzRprLck2hBjwPibuat2nOLJ1l4ZagsqVW-mojxdCtme0MIKYWPebYnK9hWnFHLSmkAYSGPyuSkYPDGcxHAHeYV0oiKQoAPL581g
v4pia32YkAjXdcncqv0amKalMA089kUcv13tZqY0pAin0iMO---5og78M0BV8RYQHP3WinvT6Jg8P7NxDpgiUK22kHv1JXj-D_EMMSLEC20Ey7ImwESpNb1vkrGHCu4iHUKN61joSkyt1vxJ6JctK7gks
qcWbtDr81e5fohnSSI5mRnysqx-WE8ZT8wrrrtTNArfkQ00g"
>> "x-ms-effective-locale"="en.en-us"
>> "Accept"="*/*"
>> "x-ms-client-request-id"="b0864d22-023e-4e77-afcf-9b36de5c7066"
[>> }

StatusCode      : 200
StatusDescription : OK
Content         : {"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users(displayName)/$entity", "displayName": "Andy Robbins"}
RawContent      : HTTP/1.1 200 OK
Cache-Control   : no-cache
Transfer-Encoding: chunked
Strict-Transport-Security: max-age=31536000
request-id: f5b23cf0-4f1e-47b3-8c0e-7a97eb1101b9
client-request-id: f5b23cf0-4f1e-47b3-8c...
Headers         : {[Cache-Control, System.String[]], [Transfer-Encoding, System.String[]], [Strict-Transport-Security, System.String[]], [request-id, System.String[]]...}
Images          : {}
InputFields     : {}
Links           : {}
RawContentLength : 119
RelationLink    : {}

PS /Users/andyrobbins> █

```

Explore the system using various means



Azure Portal GUI



MS-authored CLI tools

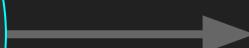
az binary
AzureAD PowerShell Module
Az PowerShell Module

```
PS C:\Users\andyrobbins> Import-Module AzureAD
PS C:\Users\andyrobbins> Get-Command -Module AzureAD
```

CommandType	Name	Version	Source
Alias	Get-AzureADApplicationProxyConnectorGroupMembers	2.0.2.140	AzureAD
Cmdlet	Add-AzureADApplicationOwner	2.0.2.140	AzureAD
Cmdlet	Add-AzureADDeviceRegisteredOwner	2.0.2.140	AzureAD
Cmdlet	Add-AzureADDeviceRegisteredUser	2.0.2.140	AzureAD
Cmdlet	Add-AzureADDirectoryRoleMember	2.0.2.140	AzureAD
Cmdlet	Add-AzureADGroupMember	2.0.2.140	AzureAD
Cmdlet	Add-AzureADGroupOwner	2.0.2.140	AzureAD
Cmdlet	Add-AzureADMSAdministrativeUnitMember	2.0.2.140	AzureAD
Cmdlet	Add-AzureADMSApplicationOwner	2.0.2.140	AzureAD
Cmdlet	Add-AzureADMSLifecyclePolicyGroup	2.0.2.140	AzureAD
Cmdlet	Add-AzureADMSScopedRoleMembership	2.0.2.140	AzureAD
Cmdlet	Add-AzureADMSServicePrincipalDelegatedPermissionC...	2.0.2.140	AzureAD
Cmdlet	Add-AzureADServicePrincipalOwner	2.0.2.140	AzureAD
Cmdlet	Confirm-AzureADDomain	2.0.2.140	AzureAD
Cmdlet	Connect-AzureAD	2.0.2.140	AzureAD
Cmdlet	Disconnect-AzureAD	2.0.2.140	AzureAD
Cmdlet	Enable-AzureADDirectoryRole	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplication	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationExtensionProperty	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationKeyCredential	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationLogo	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationOwner	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationPasswordCredential	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationProxyApplication	2.0.2.140	AzureAD
Cmdlet	Get-AzureADApplicationProxyApplicationConnectorGr...	2.0.2.140	AzureAD

```
105     function Invoke-AzureHound {
106         [CmdletBinding()]
107         Param(
108             [Parameter(Mandatory=$False)][String]$TenantID = $null,
109             [Parameter(Mandatory=$False)][String]$OutputDirectory = $(Get-Location), [ValidateNotNullOrEmpty()])
110             [Parameter(Mandatory=$False)][Switch]$Install = $null)
111
112         if ($Install){
113             Install-Module -Name Az -AllowClobber
114             Install-module -Name AzureADPreview -AllowClobber
115         }
116
117         $Modules = Get-InstalledModule
118         if ($Modules.Name -notcontains 'Az.Accounts' -and $Modules.Name -notcontains 'AzureAD'){
119             Write-Host "AzureHound requires the 'Az' and 'Azure AD PowerShell module, please install by using the -Install switch."
120             exit
121         }
122
123         $date = get-date -f yyyyMMddhhmmss
124
125         #Login Check
126         $APSUser = Get-AzContext *>&1
127         if ($APSUser -eq $null){
128             Connect-AzAccount
129             $APSUser = Get-AzContext *>&1
130             if ($APSUser -eq $null){
131                 Write-Host "Login via Az PS Module failed."
132                 exit
133             }
134         }
135         Connect-AADUser
136         $Headers = Get-AzureGraphToken
137
138         If(!$TenantID){
139             $TenantObj = Invoke-RestMethod -Headers $Headers -Uri 'https://graph.microsoft.com/beta/organization'
140             $Tenant = $TenantObj.value
141             $TenantId = $Tenant.id
142         }
143
144         # Enumerate users
145         $Coll = New-Object System.Collections.ArrayList
146         Write-Info "Building users object, this may take a few minutes."
147             $AADUsers = Get-AzureADUser -All $True | Select UserPrincipalName,OnPremisesSecurityIdentifier,objectId,TenantId
```

Explore the
system using
various means



Azure Portal GUI

MS-authored CLI tools

Our own basic client

```
1 $Body = @{
2     Grant_Type      = "client_credentials"
3     Scope           = "https://graph.microsoft.com/.default"
4     Client_Id       = "5cb4d011-ef3d-4c4a-afe4-1189dd1808ae"
5     Client_Secret   = "3qh7Q~WIbzpawgeIeOu1QKA~.VPMBWK3vIgpU"
6 }
7 $Token = Invoke-RestMethod `n
8     -URI          "https://login.microsoftonline.com/specterdev.onmicrosoft.com/oauth2/v2.0/token" `n
9     -Method        POST `n
10    -Body          $Body `n
11 `n
12 # List users in my tenant
13 $Users = Invoke-RestMethod `n
14     -Headers      @{Authorization = "Bearer $($Token.access_token)" } `n
15     -Uri          "https://graph.microsoft.com/v1.0/users/" `n
16     -Method        GET `n
17 `n
18 $Users.value
```

Get a token

Get data
from the API

Work with
the data

Client execution

```
PS /Users/andyrobbins> $Body = @{
>>     Grant_Type      = "client_credentials"
>>     Scope           = "https://graph.microsoft.com/.default"
>>     client_Id       = "5cb4d011-ef3d-4c4a-afe4-1189dd1808ae"
>>     Client_Secret   = "3qh7Q~WIBzpawgelEoU1QKA~.VPMBWK3vIgpU"
>> }
PS /Users/andyrobbins> $Token = Invoke-RestMethod ` 
>>     -URI          "https://login.microsoftonline.com/specterdev.onmicrosoft.com/oauth2/v2.0/token" ` 
>>     -Method        POST ` 
>>     -Body          $Body
PS /Users/andyrobbins>
PS /Users/andyrobbins> # List users in my tenant
PS /Users/andyrobbins> $Users = Invoke-RestMethod ` 
>>     -Headers        @{"Authorization" = "Bearer $($Token.access_token)" } ` 
>>     -Uri           "https://graph.microsoft.com/v1.0/users/" ` 
>>     -Method        GET
PS /Users/andyrobbins>
PS /Users/andyrobbins> $Users.value | Select -First 2
```

```
businessPhones    : {}
displayName       : Andrew Chiles
givenName         : Andrew
jobTitle          : Simulation
mail              : achiles@specterdev.onmicrosoft.com
mobilePhone       :
officeLocation    :
preferredLanguage :
surname           : Chiles
userPrincipalName : achiles@specterdev.onmicrosoft.com
id                : d17d05dd-cbe9-41de-ac4d-93df58de0792

businessPhones    : {}
displayName       : Andy Robbins
givenName         : Andy
jobTitle          :
mail              :
mobilePhone       :
officeLocation    :
preferredLanguage :
surname           : Robbins
userPrincipalName : arobbins@specterdev.onmicrosoft.com
id                : 16571a9f-a0b4-476a-87e8-14dca511b9a3

PS /Users/andyrobbins>
```

The data

```
1 $Body = @{
2     Grant_Type      = "client_credentials"
3     Scope           = "https://graph.microsoft.com/.default"
4     Client_Id       = "5cb4d011-ef3d-4c4a-afe4-1189dd1808ae"
5     Client_Secret   = "3qh7Q~WIbzpawgelEoU1QKA~.VPMBWK3vIgpU"
6 }
7 $Token = Invoke-RestMethod ` 
8     -URI          "https://login.microsoftonline.com/specterdev.onmicrosoft.com/oauth2/v2.0/token" ` 
9     -Method        POST ` 
10    -Body          $Body
11
12 # Get list of our test service principals by their ID
13 $URI = "https://graph.microsoft.com/v1.0/users"
14 $Results = $null
15 $Users = $null
16 do {
17     $Results = Invoke-RestMethod ` 
18         -Headers @{Authorization = "Bearer $($Token.access_token)"} ` 
19         -URI $URI ` 
20         -UseBasicParsing ` 
21         -Method "GET" ` 
22         -ContentType "application/json"
23     if ($Results.value) {
24         $TestSPObjects += $Results.value
25     } else {
26         $TestSPObjects += $Results
27     }
28     $uri = $Results.'@odata.nextlink'
29 } until (!$uri)
30
```

Token gotchas

- JWTs facilitate stateless authentication but only **partly** facilitate stateless authorization
- But not all authorization is stored in the JWT

Token gotchas

- JWTs facilitate stateless authentication but only **partly** facilitate stateless authorization
- But not all authorization is stored in the JWT
- AzureAD roles and MS Graph roles are stored in JWTs
- But these tokens do not include AzureRM role assignments or the various other access control configs

Token gotchas

- JWTs facilitate stateless authentication but only **partly** facilitate stateless authorization
- But not all authorization is stored in the JWT
- AzureAD roles and MS Graph roles are stored in JWTs
- But these tokens do not include AzureRM role assignments or the various other access control configs
- Tl;dr: You can have **more privileges** than what your JWT states

```
1 # Get a token for MS Graph API as the "MyCoolApp" service principal
2 $clientId      = "4a2d703b-ec39-4fe4-98a9-e298d5a0f540"
3 $tenantName    = "specterdev.onmicrosoft.com"
4 $clientSecret  = "PYi7Q~LCQu5LChhdUYU9rMjYDQModARxDa00"
5 $resource      = "https://graph.microsoft.com/"
6
7 $Body = @{
8     Grant_Type      = "client_credentials"
9     Scope           = "https://graph.microsoft.com/.default"
10    client_Id       = $clientID
11    Client_Secret   = $clientSecret
12 }
13
14 $token = Invoke-RestMethod ` 
15     -Uri          "https://login.microsoftonline.com/$TenantName/oauth2/v2.0/token" ` 
16     -Method        POST ` 
17     -Body          $Body
18
19 # $token.access_token is our bearer token
20 $token.access_token
21
22 # Now that we have a bearer token, we can interface with the MS Graph API
23 $URI          = 'https://graph.microsoft.com/v1.0/Groups/'
24 $Request      = Invoke-RestMethod ` 
25     -Headers @{'Authorization = "Bearer $($token.access_token)"} ` 
26     -URI $URI ` 
27     -Method GET
28 $Request.value | Select -First 1
```

```
PS C:\Users\andyrobbins> # Get a token for MS Graph API as the "MyCoolApp" service principal
PS C:\Users\andyrobbins> $clientId      = "4a2d703b-ec39-4fe4-98a9-e298d5a0f540"
PS C:\Users\andyrobbins> $tenantName    = "specterdev.onmicrosoft.com"
PS C:\Users\andyrobbins> $clientSecret  = "PYi7Q~LCQu5LChhdUYU9rMjYDQModARxDa00"
PS C:\Users\andyrobbins> $resource      = "https://graph.microsoft.com/"
PS C:\Users\andyrobbins>
PS C:\Users\andyrobbins> $Body = @{
>>   Grant_Type      = "client_credentials"
>>   Scope           = "https://graph.microsoft.com/.default"
>>   client_Id       = $clientId
>>   Client_Secret   = $clientSecret
>> }
PS C:\Users\andyrobbins>
PS C:\Users\andyrobbins> $token = Invoke-RestMethod ` 
>>   -Uri          "https://login.microsoftonline.com/$TenantName/oauth2/v2.0/token" ` 
>>   -Method        POST ` 
>>   -Body          $Body
PS C:\Users\andyrobbins>
PS C:\Users\andyrobbins> # $token.access_token is our bearer token
PS C:\Users\andyrobbins> $token.access_token
eyJ0eXAiOiJKV1QiLCJub25jZSI6Im5xRVdUQjZMOVJWcjNIY0RRaVA2VmpWaTFFeHFrcGlkRkhUHBtUkFfVHciLCJhbGciOiJSUzI1NiIsIng1dCI6Ik1y
NS1BVWlizkJpaTd0ZDFqQmViYXhib1hXMCIsImtpZCI6Ik1yNS1BVWlizkJpaTd0ZDFqQmViYXhib1hXMCJ9.eyJhdWQiOiJodHRwczovL2dyYXB0Lm1pY3J
vc29mdC5jb20iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC82YzEyYjBiMC1iMmNjLTrhNzMtODI1Mi0wYjk0YmZjYTIXNDUvIiwiWF0IjoxNjQ
1NTcwNTU3LCJuYmYiOjE2NDU1NzA1NTcsImV4cCI6MTY0NTU3NDQ1NywiYWlvIjoiRTJaZ1lPQXhiNzNTVnUvMzMbXhxFVZ2bmRKL0FBPT0iLCJhcHBfZG1
zcGxheW5hbWUiOijNeUNvb2xBcHAIcJhcHBpZCI6IjRhMmQ3MDNiiLWvjMzktnGZlNC050GE5LWUyOTHkNWxEwzju0MCIsImFwcGlkYWNyIjoiMSIsImlkccCI
6Imh0dHBz0i8vc3RzLndpbmRvd3Mu bmV0LzzjMTJiMGIwLWIyY2MtNGE3My04MjUyLTBi0TRiZmNhMjE0NS8iLCJpZHR5cCI6ImFwcCIsIm9pZCI6ImQxNDY
0NjRmLTUyM2EtNGQyNC1iZmNLLTE3ZDIxNTY4NjQ3ZSiSInJoIjoiMC5BvkVBc0xBU2JNxLjMHFDVWd1VXY4b2hSUU1BQUFBQUFBQUFBQLj
BQUEUiIwicm9sZXMi0lsirGlyZWN0b3J5L1J1YQuQWxsIl0sInN1YiI6ImQxNDY0NjRmLTUyM2EtNGQyNC1iZmNLLTE3ZDIxNTY4NjQ3ZSiSInRlbmFudF9
yzWdpb25fc2NvcGUiOijQOSiSInRpZCI6IjZjMTJiMGIwLWIyY2MtNGE3My04MjUyLTBi0TRiZmNhMjE0NSiSInV0aSI6IkExSWFrWk9CVFV5czRzTndQSEF
UQWciLCJ2ZXii0iIxLjAiLCJ3aWRzIjpbiJAS0TdhMWQwLTBKMWQtNGFjYi1iNDA4LWQ1Y2E3MzEyMWU5MCJdLCJ4bXNfdGNkdCI6MTU4ODYwMjg3M30.rwl
1jDm5z1EH3QVCiva6Fd1z-FSpw6VZpFGohETT-gJLY0LiMFTJwi8f9ghl4XUgiQGbazFMfx85-xbaPerbHGW3dCjFh1EfXXloLXB8TJ9GTvrJNGa0jX2Xj5
T6tAYUp75ci06BxPF8eXH0a-7f0q24hhKwcqG5QXhMkg4Dv5mtzQ7yrA4W0FzczXbPKALFq5Xz579zJyvfRAeNup_TkVv6s4h_eLeNa-dzxSvq80uTXD7gmw
1dFAcvf4rJARgpGRml1aR50bePbvdQUCpHWikgZGB7AI4ovjmLcGueK0jZdAmDVjo7li93T1A0xf6UV9SJddk74bX7224DFi9zw
PS C:\Users\andyrobbins>
```

```
eyJ0eXAiOiJKV1QiLCJub25jZSI6Im5xRvduQjZMOVJWcjNlY0RRaVA2VmpWaTFFeHFrcGlkRkhIUHbtUKFFvHciLCJhbGciOiJSUzI1NiIsIngldCI6Ik1yNS1BvWliZkJpatdoZDFqMvIYXhib1hXMCIsImtpZCI6Ik1yNS1BvWliZkJpaTdoZDFqMvIYXhib1hXMCJ9.eyJhdWQiOiJodHRwczovL2dyYXB0Lm1pY3Jvc29mdC5jb20iLCJpc3M1oIjodHRwczovL3N0cy53aw5kb3dzLm5ldc82YzEyjB1MC1iMmNjLTrhNzMtODI1Mi0wYjk0mzYTIXNDUvIwiawF0IjoxNjQ1NTcwNTU3LCJuYm1oje2NDU1Nza1NTcsImV4cCI6MTY0NTU3NDQ1NyiwIYwlvjoiRTJaZ1lPQXhiNzNTNvUmZBMBxhxRVZ2bmRKL0FBPT0iLCJhcHBfZG1zcGxhe5hbWUj01JNeUNvb2x8CHAI1C3hchBpzC16IjRhMmQ3MDN1lLWVjm2ktNGz1NC050GE5LWuY0ThkNWEwZjU0MC1sImFwcG1kYWhnYIjoiMSisIm1kCC16Imh0dHBzoi8vc3RzLndpbmRvd3Mu bmV0LzjMTJ1MGiwlWIyY2MtNGE3My04MjuyLTBi0TRizmNhMjE0NS8iLCJpZHR5cCI6ImFwcCIsIn9pZCI6ImQxNDY0NjRmlTUyM2tENGQyNC1zmn1LTE3ZDIXNTY4NjQ3ZSIsInJ0IjoiMC5BvkVbc0xBU2JNx1jMHFDVwd1VXY4b2HSUu1BQUFBQUFBQUFBQUFBQ1JBQUEuIiwi cms sZXM1ols1RgLyZWNob335L1j1YwQuQWxs1l0sInh1Yi6ImQxNDY0NjRmlTUyM2tENGQyNC1zmn1LTE3ZDIXNTY4NjQ3ZSIsInRlbfudF9yZwdpb25fc2NvcGUiOjJOQSiSInRpZCI6IjZjMTJ1MGiwlWIyY2MtNGE3My04MjuyLTBi0TRizmNhMjE0NS1sInV0aSI6IkExSWFrWk9CVFV5czRzTndQSEFUQWciLCJ2ZXii0iXljA1LCJ3aWRzIjpbIjA50TdhMWQwLTbkmWQtNGfjy1iINDA4LwQ1Y2E3MzEyMWU5MCJdLCJ4bXNfdGNkdCI6MTU40DYwMjg3M30.rW11jDm5z1EH3QQVCivaFd1z-FSpw6VzpFG0hETT-gJY0LiMfTJwi8f9gh14XUgiQGba zFMfx85-xbaPerbHGW3dCjFh1EfXXloLXB8TJ9GTvrJNGa0jX2Xj5T6tAYUp75ci06BxPF8eXH0a-7f0q24hhWkcG5QXhMkg4Dv5mtzQ7yrA4W0Fz2xPbPKALFq5Xz579zJyvfRAeNup_TkVv6s4h_eLEnA-dzxSvq80uTXD7gmu1dFAcVf4rJARgpGRml1aR50bePbv dQUCPbWikgZGB7AI4ovjmLcGueK0jZdAmDVjo7li93T1Ax0xf6UV9SJddk74bX7224DF19zw
```

This token was issued by [Azure Active Directory](#).

Decoded Token

Claims

```
{
  "typ": "JWT",
  "nonce": "nqEWTB6L9RVr3HcDQiP6VjVi1ExqkpidFhbPpmRA_Tw",
  "alg": "RS256",
  "x5t": "Mr5-AUibfBii7Nd1jBebaxboXw0",
  "kid": "Mr5-AUibfBii7Nd1jBebaxboXw0"
}.{
  "aud": "https://graph.microsoft.com",
  "iss": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/",
  "iat": 1645570557,
  "nbf": 1645570557,
  "exp": 1645574457,
  "aio": "E2ZgYOAx b73SVu/30LmxqEVvn dJ/AA==",
  "app_displayname": "MyCoolApp",
  "appid": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540",
  "appidacr": "1",
  "idp": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/",
  "idtyp": "app",
  "oid": "d146464f-523a-4d24-bfce-17d21568647e",
  "rh": "0.AVEASLASbMyyc0qCuguJv8ohRQMaaaaaaaaaaaaAAAABRAAA.",
  "roles": [
    "Directory.Read.All"
  ],
}
```

Audience

Decoded Token	Claims
	<pre>{ "typ": "JWT", "nonce": "nqEWTB6L9RVr3HcDQiP6VjVi1ExqkpidFHbPpmRA_Tw", "alg": "RS256", "x5t": "Mr5-AUibfBii7Nd1jBebaxboXW0", "kid": "Mr5-AUibfBii7Nd1jBebaxboXW0" }.{ "aud": "https://graph.microsoft.com", "iss": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "iat": 1645570557, "nbf": 1645570557, "exp": 1645574457, "aio": "E2ZgYOAx73SVu/30LmxqEVvndJ/AA==", "app_displayname": "MyCoolApp", "appid": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540", "appidacr": "1", "idp": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "idtyp": "app", "oid": "d146464f-523a-4d24-bfce-17d21568647e", "rh": "0.AVEAsLASbMyyc0qCUGuUv8ohRQMAAAAAAAAABRAAA.", "roles": ["Directory.Read.All"], "sub": "d146464f-523a-4d24-bfce-17d21568647e", "tenant_region_scope": "NA", "tid": "6c12b0b0-b2cc-4a73-8252-0b94bfca2145", "uti": "A1IakZ0BTUys4sNwPHATag", "ver": "1.0", "wids": ["0997a1d0-0d1d-4acb-b408-d5ca73121e90"], "xms_tcdt": 1588602873 }.[Signature]</pre>

Decoded Token	Claims
	<pre>{ "typ": "JWT", "nonce": "nqEWTB6L9RVr3HcDQiP6VjVi1ExqkpidFHbPpmRA_Tw", "alg": "RS256", "x5t": "Mr5-AUibfBii7Nd1jBebaxboXW0", "kid": "Mr5-AUibfBii7Nd1jBebaxboXW0" }.{ "aud": "https://graph.microsoft.com", "iss": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "iat": 1645570557, "nbf": 1645570557, "exp": 1645574457, "aio": "E2ZgYOAx73SVu/30LmxqEVvndJ/AA==", "app_displayname": "MyCoolApp", "appid": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540", "appidacr": "1", "idp": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "idtyp": "app", "oid": "d146464f-523a-4d24-bfce-17d21568647e", "rh": "0.AVEAsLASbMyyc0qCUGuUv8ohRQMAAAAAAAAABRAAA.", "roles": ["Directory.Read.All"], "sub": "d146464f-523a-4d24-bfce-17d21568647e", "tenant_region_scope": "NA", "tid": "6c12b0b0-b2cc-4a73-8252-0b94bfca2145", "uti": "A1IakZ0BTUys4sNwPHATag", "ver": "1.0", "wids": ["0997a1d0-0d1d-4acb-b408-d5ca73121e90"], "xms_tcdt": 1588602873 }.[Signature]</pre>

MS Graph
scoped App
Roles

Decoded Token	Claims
	{ "typ": "JWT", "nonce": "nqEWTB6L9RVr3HcDQiP6VjVi1ExqkpidFHbPpmRA_Tw", "alg": "RS256", "x5t": "Mr5-AUibfBii7Nd1jBebaxboXW0", "kid": "Mr5-AUibfBii7Nd1jBebaxboXW0" }.{ "aud": "https://graph.microsoft.com", "iss": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "iat": 1645570557, "nbf": 1645570557, "exp": 1645574457, "aio": "E2ZgYOAx73SVu/30LmxqEVvndJ/AA==", "app_displayname": "MyCoolApp", "appid": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540", "appidacr": "1", "idp": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/", "idtyp": "app", "oid": "d146464f-523a-4d24-bfce-17d21568647e", "rh": "0.AVEAsLASbMyyc0qCUGuUv8ohRQMAAAAAAAAABRAAA.", "roles": ["Directory.Read.All"], "sub": "d146464f-523a-4d24-bfce-17d21568647e", "tenant_region_scope": "NA", "tid": "6c12b0b0-b2cc-4a73-8252-0b94bfca2145", "uti": "A1IakZ0BTUys4sNwPHATag", "ver": "1.0", "wids": ["0997a1d0-0d1d-4acb-b408-d5ca73121e90"], "xms_tcdt": 1588602873 . [Signature]

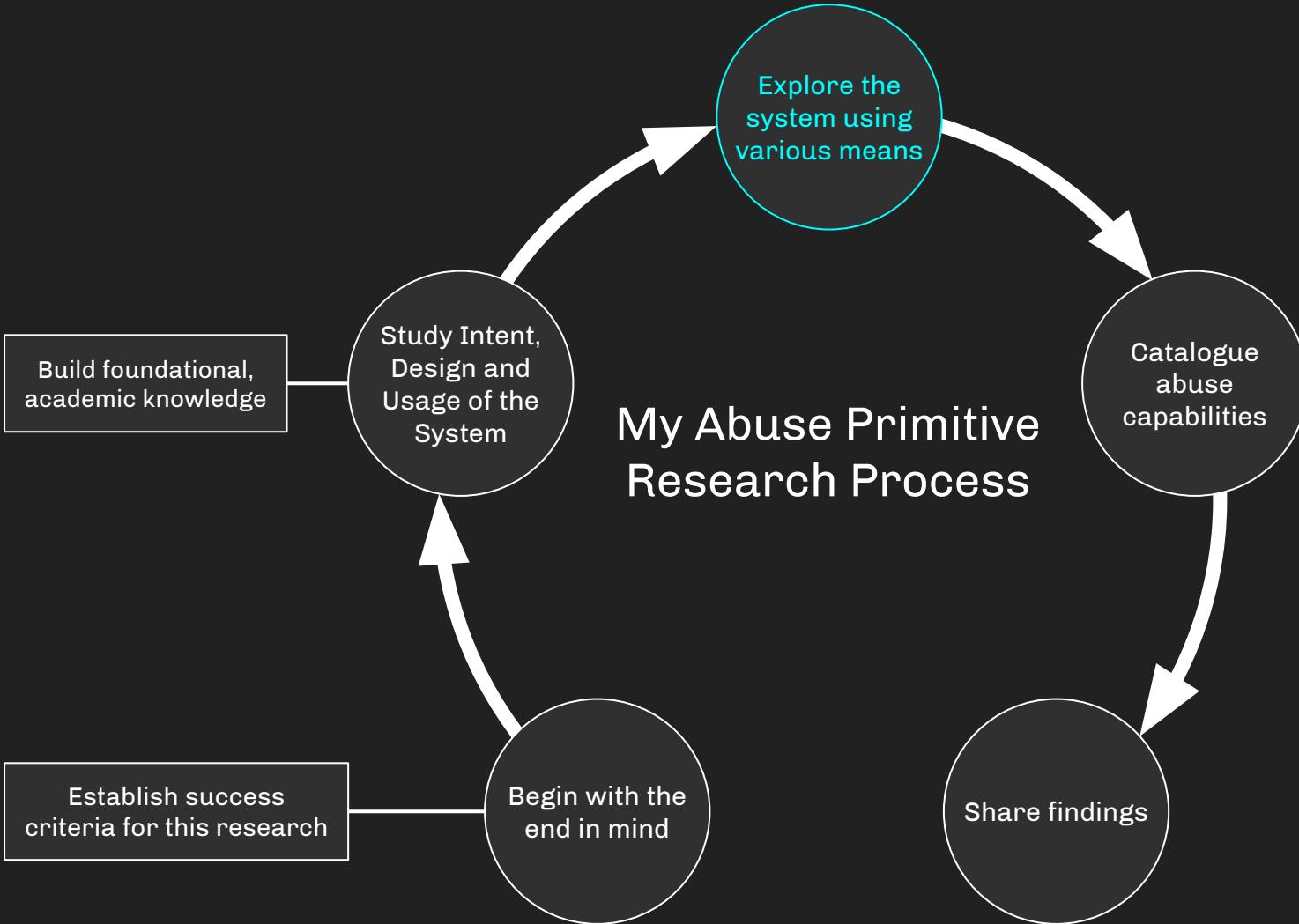
Decoded Token Claims

```
{  
    "typ": "JWT",  
    "nonce": "nqEWTB6L9RVr3HcDQiP6VjVi1ExqkpidFHbPpmRA_Tw",  
    "alg": "RS256",  
    "x5t": "Mr5-AUibfBii7Nd1jBebaxboXW0",  
    "kid": "Mr5-AUibfBii7Nd1jBebaxboXW0"  
}.{  
    "aud": "https://graph.microsoft.com",  
    "iss": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/",  
    "iat": 1645570557,  
    "nbf": 1645570557,  
    "exp": 1645574457,  
    "aio": "E2ZgYOAx73SVu/30LmxqEVvndJ/AA==",  
    "app_displayname": "MyCoolApp",  
    "appid": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540",  
    "appidacr": "1",  
    "idp": "https://sts.windows.net/6c12b0b0-b2cc-4a73-8252-0b94bfca2145/",  
    "idtyp": "app",  
    "oid": "d146464f-523a-4d24-bfce-17d21568647e",  
    "rh": "0.AVEAsLASbMyyc0qCUGuUv8ohRQMAAAAAAAAABRAAA.",  
    "roles": [  
        "Directory.Read.All"  
    ],  
    "sub": "d146464f-523a-4d24-bfce-17d21568647e",  
    "tenant_region_scope": "NA",  
    "tid": "6c12b0b0-b2cc-4a73-8252-0b94bfca2145",  
    "uti": "A1IakZ0BTUys4sNwPHATag",  
    "ver": "1.0",  
    "wids": [  
        "0997a1d0-0d1d-4acb-b408-d5ca73121e90"  
    ],  
    "xms_tcdt": 1588602873  
}.[Signature]
```

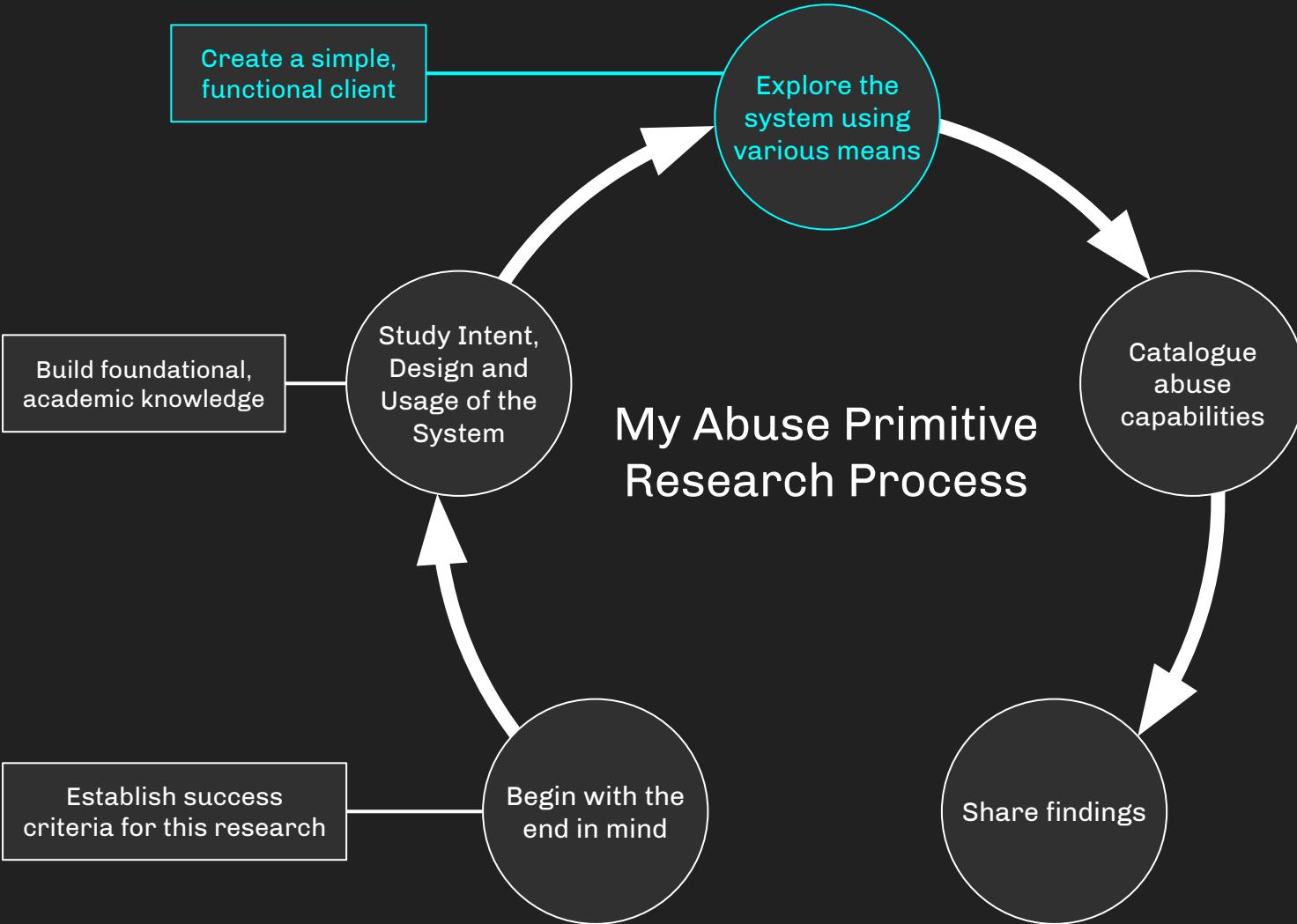
AzureAD Roles



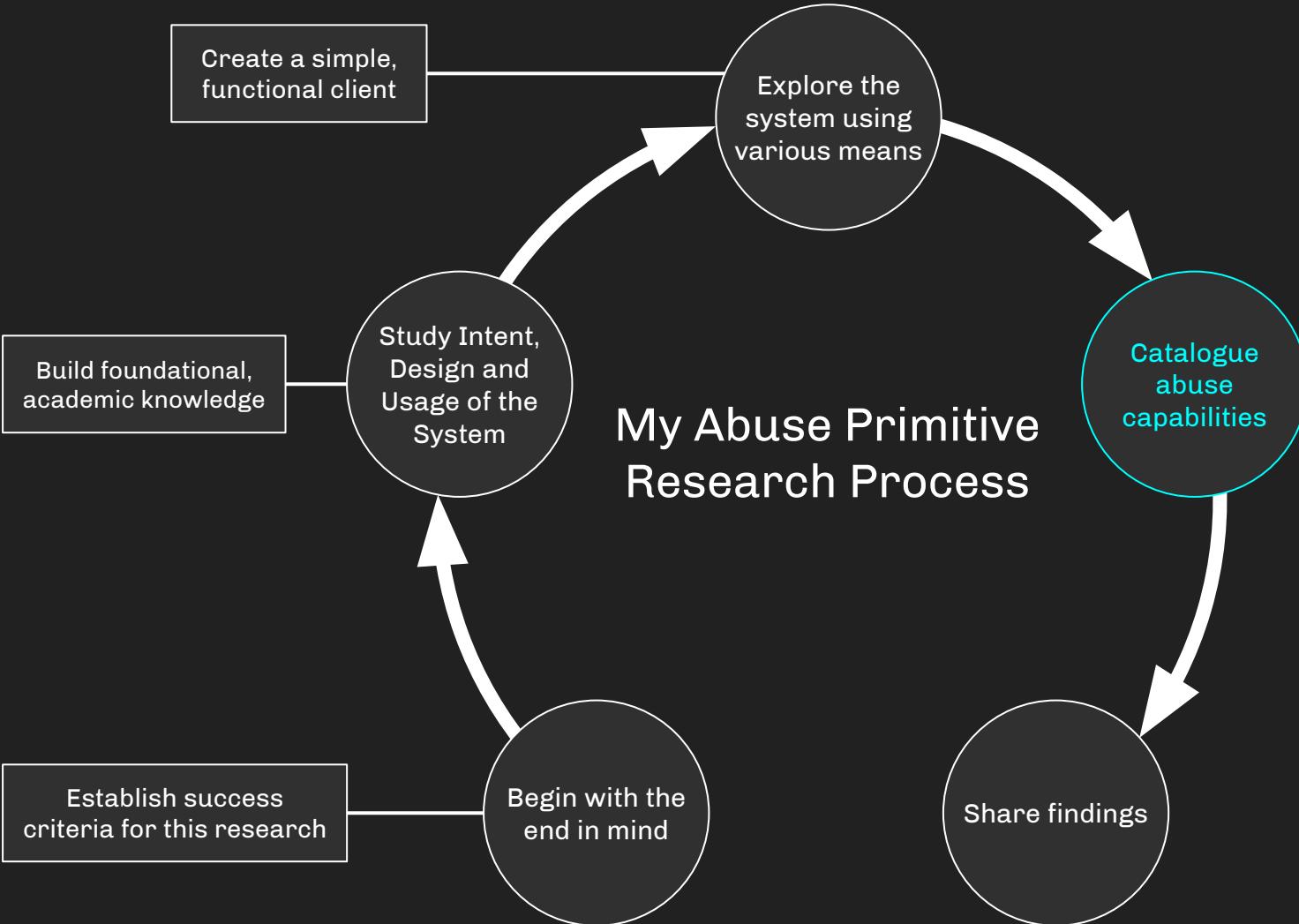
My Abuse Primitive Research Process



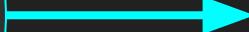
My Abuse Primitive Research Process



My Abuse Primitive Research Process



Catalogue
abuse
capabilities



Enumerate assignable
permissions

```
30 # Collect all service principal objects and put them into $ServicePrincipals
31 $URI = "https://graph.microsoft.com/v1.0/servicePrincipals"
32 $Results = $null
33 $ServicePrincipals = $null
34 do {
35     $Results = Invoke-RestMethod ` 
36         -Headers @{Authorization = "Bearer $($token.access_token)" } ` 
37         -URI $URI ` 
38         -UseBasicParsing ` 
39         -Method "GET" ` 
40         -ContentType "application/json"
41     if ($Results.value) {
42         $ServicePrincipals += $Results.value
43     } else {
44         $ServicePrincipals += $Results
45     }
46     $uri = $Results.'@odata.nextlink'
47 } until (!$uri)
```



C:\Users\andyrobbins\AppData\



```
PS C:\Users\andyrobbins> $ServicePrincipals | ?{$_appId -Match '00000000-0000-0000-0000-000000000000'}  
appRoles | sort-object -property value | select value
```

value

AccessReview.Read.All
AccessReview.ReadWrite.All
AccessReview.ReadWrite.Membership
AdministrativeUnit.Read.All
AdministrativeUnit.ReadWrite.All
Agreement.Read.All
Agreement.ReadWrite.All
AgreementAcceptance.Read.All
APIConnectors.Read.All
APIConnectors.ReadWrite.All
AppCatalog.Read.All
AppCatalog.ReadWrite.All
Application.Read.All
Application.ReadWrite.All
Application.ReadWrite.OwnedBy
AppRoleAssignment.ReadWrite.All
AuditLog.Read.All

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPIdIJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

A1

	A	B	C	D
1				
2	value			
3	----			
4	AccessReview.Read.All			
5	AccessReview.ReadWrite.All			
6	AccessReview.ReadWrite.Membership			
7	AdministrativeUnit.Read.All			
8	AdministrativeUnit.ReadWrite.All			
9	Agreement.Read.All			
10	Agreement.ReadWrite.All			
11	AgreementAcceptance.Read.All			
12	APIConnectors.Read.All			
13	APIConnectors.ReadWrite.All			
14	AppCatalog.Read.All			
15	AppCatalog.ReadWrite.All			
16	Application.Read.All			
17	Application.ReadWrite.All			
18	Application.ReadWrite.OwnedBy			
19	AppRoleAssignment.ReadWrite.All			
20	AuditLog.Read.All			
21	BitlockerKey.Read.All			
22	BitlockerKey.ReadBasic.All			
23	Calendars.Read			
24	Calendars.ReadWrite			
25	CallRecord-PstnCalls.Read.All			

Catalogue
abuse
capabilities

Enumerate assignable
permissions

Test existing abuses,
consider new abuses

Application permissions

Permission	Display String	Description	Admin Consent Required
<i>Directory.Read.All</i>	Read directory data	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	Yes
<i>Directory.ReadWrite.All</i>	Read and write directory data	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.	Yes



100%

\$

%

.0

.00

123

Default (Ari...

10

B

I

S

A



D1



Add Principal to Role Enabled Security Group

	A	B	C	D
1	MS Graph App Role Name	Promote Self to Global Admin	Change Global Admin's Password	Add Principal to Role Enabled Se
2	----			
3	AccessReview.Read.All			
4	AccessReview.ReadWrite.All			
5	AccessReview.ReadWrite.Membership			
6	AdministrativeUnit.Read.All			
7	AdministrativeUnit.ReadWrite.All			
8	Agreement.Read.All			
9	Agreement.ReadWrite.All			
10	AgreementAcceptance.Read.All			
11	APIConnectors.Read.All			
12	APIConnectors.ReadWrite.All			
13	AppCatalog.Read.All			
14	AppCatalog.ReadWrite.All			
15	Application.Read.All			
16	Application.ReadWrite.All			
17	Application.ReadWrite.OwnedBy			
18	AppRoleAssignment.ReadWrite.All			
19	AuditLog.Read.All			
20	BitlockerKey.Read.All			
21	BitlockerKey.ReadBasic.All			
22	Calendars.Read			
23	Calendars.ReadWrite			
24	CallRecord-PstnCalls.Read.All			
25	CallRecords.Read.All			

MyCoolApp | API permissions

Search (Cmd+/)



Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Request API permissions

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

Start typing a permission to filter these results

Permission Admin consent required

AccessReview (1)

Permission	Admin consent required
<input checked="" type="checkbox"/> AccessReview.Read.All ⓘ Read all access reviews	Yes
<input type="checkbox"/> AccessReview.ReadWrite.All ⓘ Manage all access reviews	Yes
<input type="checkbox"/> AccessReview.ReadWrite.Membership ⓘ Manage access reviews for group and app memberships	Yes

> AdministrativeUnit

> AgreementAcceptance

> Agreement

> APIConnectors

> AppCatalog

Add permissions

Discard

Version

Microsoft Graph REST API v1.0

Filter by title

- > Organizational contacts
- ✓ Role management
 - Role management
 - > Role definition
 - ✓ Role assignment
 - Role assignment
 - List
 - Create**
 - Get
 - Delete
 - > Identity and sign-in
 - > Governance
- > Mail
- > Notes

Example 1: Create a role assignment with a tenant-wide scope

Request

The following is an example of the request. Note the use of the `roleTemplateId` for `roleDefinitionId`. `roleDefinitionId` can be either the service-wide template Id or the directory-specific `roleDefinitionId`.

HTTP C# JavaScript Objective-C Java Go PowerShell

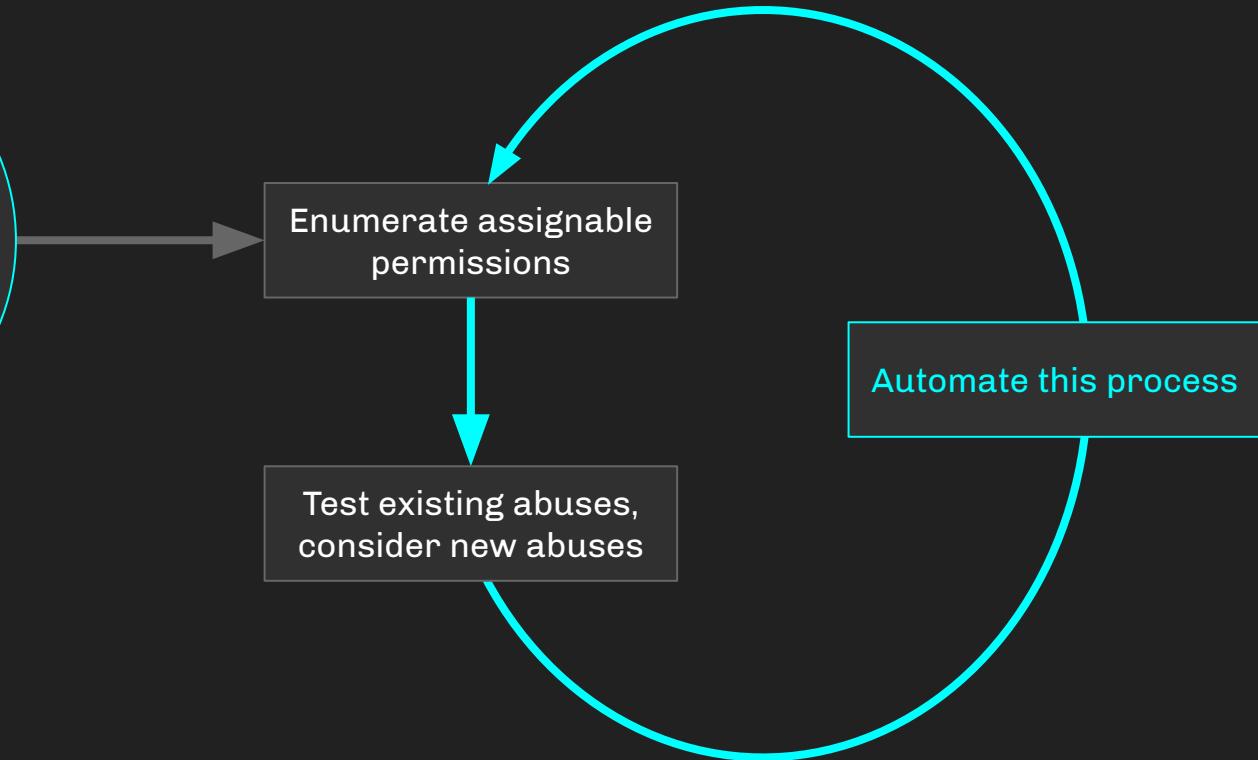
HTTP 

```
POST https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments
Content-type: application/json

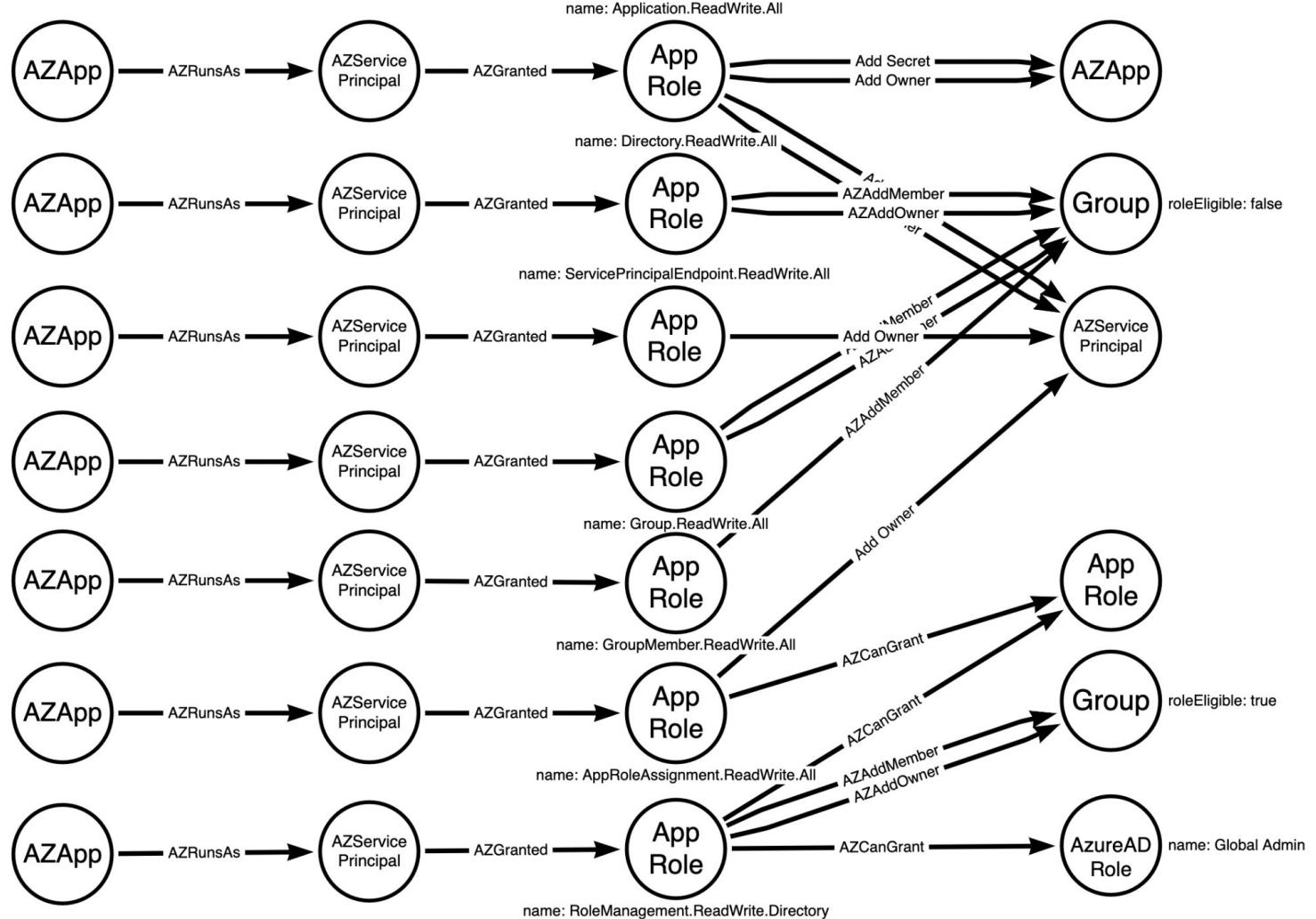
{
    "@odata.type": "#microsoft.graph.unifiedRoleAssignment",
    "roleDefinitionId": "c2cf284d-6c41-4e6b-afac-4b80928c9034",
    "principalId": "f8ca5a85-489a-49a0-b555-0a6d81e56f0d",
    "directoryScopeId": "/"
}
```

```
PS C:\Users\andyrobbins> # Try to grant "MyCoolApp" the "Global Admin" role:
PS C:\Users\andyrobbins> $body = @{
>>   "@odata.type" = "#microsoft.graph.unifiedRoleAssignment"
>>   principalId = "d146464f-523a-4d24-bfce-17d21568647e"
>>   roleDefinitionId = "62e90394-69f5-4237-9190-012177145e10"
>>   directoryScopeId = "/"
>> }
PS C:\Users\andyrobbins> $req = $null
PS C:\Users\andyrobbins> $req = Invoke-RestMethod -Headers @{Authorization = "Bearer $($token.access_token)" } ` 
>>   -Uri "https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments" ` 
>>   -Method POST ` 
>>   -Body $($body | ConvertTo-Json) ` 
>>   -ContentType 'application/json'
Invoke-RestMethod : The remote server returned an error: (403) Forbidden.
At line:1 char:8
+ $req = Invoke-RestMethod -Headers @{Authorization = "Bearer $($token. ...
+ ~~~~~
+ CategoryInfo          : InvalidOperationException: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-RestMethod], WebExc
eption
+ FullyQualifiedErrorCode : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeRestMethodCommand
```

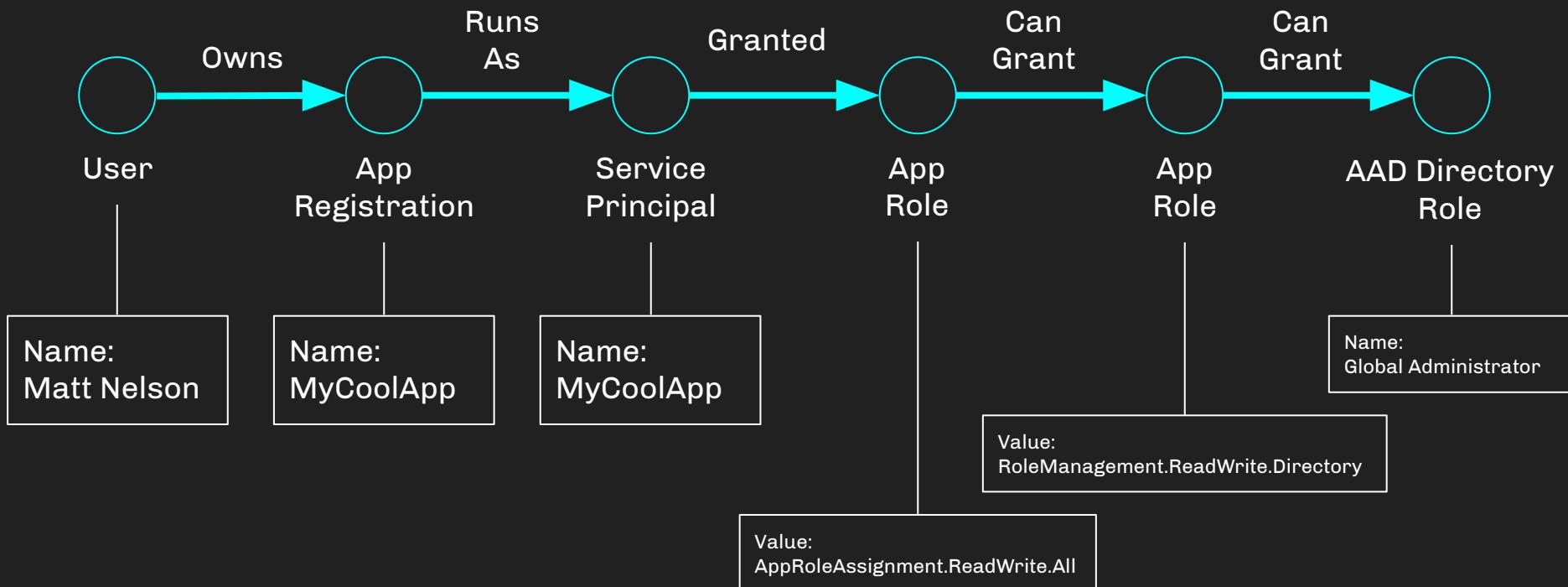

Catalogue abuse capabilities



A	B	C	D	E	F	G	H	I	J	K	L	M	N
Is that app permission abusable?													
	Abuses												
	Groups				Service Principals / Apps				Directory Roles		App Roles		
	Add owner to role eligible group	Add member to role-eligible group	Add member to non-role eligible group	Add owner to non role-eligible group	Add secret to SP	Add owner to SP	Add secret to App Reg	Add Owner to App Reg	Promote a user to Global Admin		Grant an app role		
Microsoft Graph API Permissions:													
Application.ReadWrite.All	No	No	No	No	Yes	Yes	Yes	Yes	No		No		
AppRoleAssignment.ReadWrite.All	No	No	No	No	No	Yes	No	No	No		Yes		
DelegatedPermissionGrant.ReadWrite.All	No	No	No	No	No	No	No	No	No		No		
Directory.ReadWrite.All	No	No	Yes	Yes	No	No	No	No	No		No		
Group.ReadWrite.All	No	No	Yes	Yes	No	No	No	No	No		No		
GroupMember.ReadWrite.All	No	No	Yes	No	No	No	No	No	No		No		
RoleManagement.ReadWrite.Directory	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes		Yes		
ServicePrincipalEndpoint.ReadWrite.All	No	No	No	No	No	Yes	No	No	No		No		



Example Attack Path



Filter by title

Microsoft identity platform documentation

Overview

What is the Microsoft identity platform?

What's new in docs?

Quickstarts

Tutorials

Samples

Concepts

> Authentication and authorization basics

> Authentication libraries

Permissions and access control

Permissions and consent

Permission types

The Microsoft identity platform supports two types of permissions: *delegated permissions* and *application permissions*.

- **Delegated permissions** are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests. The app is delegated with the permission to act as a signed-in user when it makes calls to the target resource.

Some delegated permissions can be consented to by nonadministrators. But some high-privileged permissions require [administrator consent](#). To learn which administrator roles can consent to delegated permissions, see [Administrator role permissions in Azure Active Directory \(Azure AD\)](#).

- **Application permissions** are used by apps that run without a signed-in user present, for example, apps that run as background services or daemons. Only an administrator can consent to application permissions.

Filter by titleMicrosoft identity platform documentationOverviewWhat is the Microsoft identity platform?What's new in docs?QuickstartsTutorialsSamplesConcepts> Authentication a> Authentication libPermissions andPermis

Permission types

The Microsoft identity platform supports two types of permissions: *delegated permissions* and *application permissions*.

- **Delegated permissions** are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests. The app is delegated with the permission to act as a signed-in user when it makes calls to the target resource.

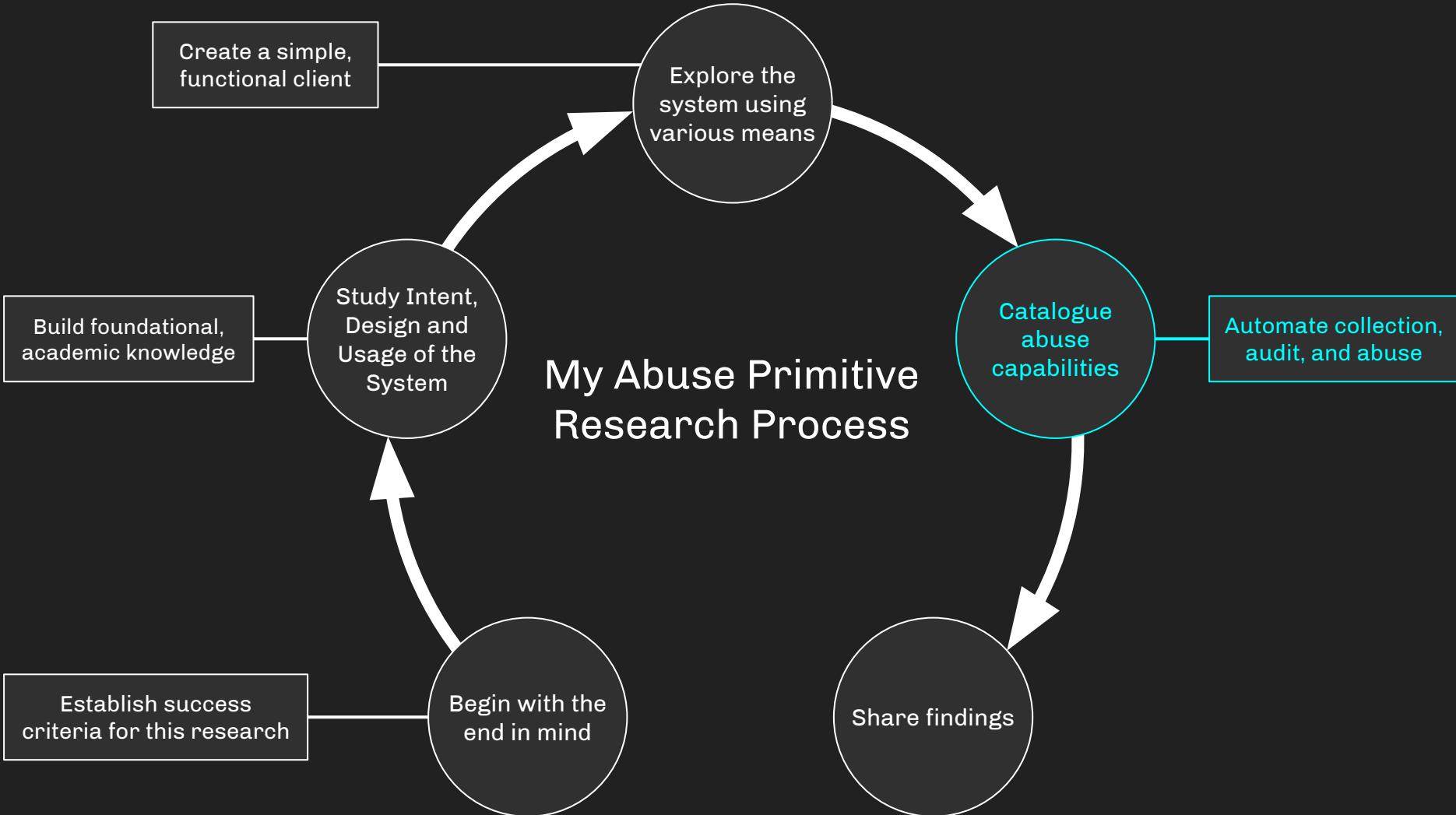
Some delegated permissions can be consented to by nonadministrators. But some high-privileged permissions require administrator consent. To learn which administrator roles can consent to delegated permissions, see Administrator role permissions in Azure Active Directory (Azure AD).

- **Application permissions** are used by apps that run without a signed-in user present, for example, apps that run as background services or daemons. Only an administrator can consent to application permissions.

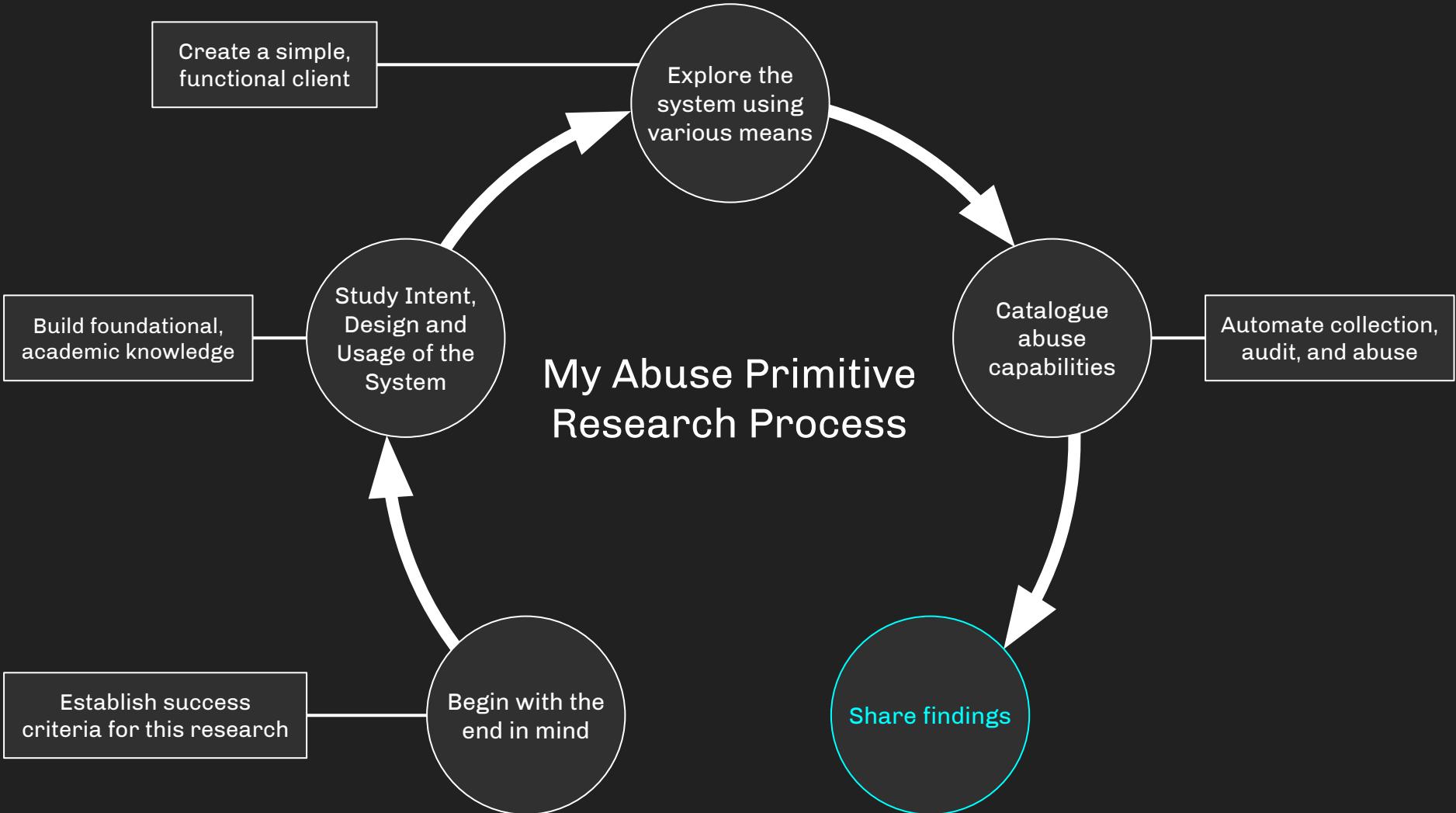
Coming soon: Atomic Azure Tests

- Inspired by Red Canary's [Atomic Red Team](#)
 - But with **no dependence** on existing PowerShell modules
 - Can be easily expanded to cover other Azure services
-
- End result: daily automatic permission->abuse mapping available for anyone to see.

My Abuse Primitive Research Process



My Abuse Primitive Research Process



```
graph TD; A((Share findings)) --> B[Write a Blog]; A --> C[Share your Code]; A --> D[Give a Talk]
```

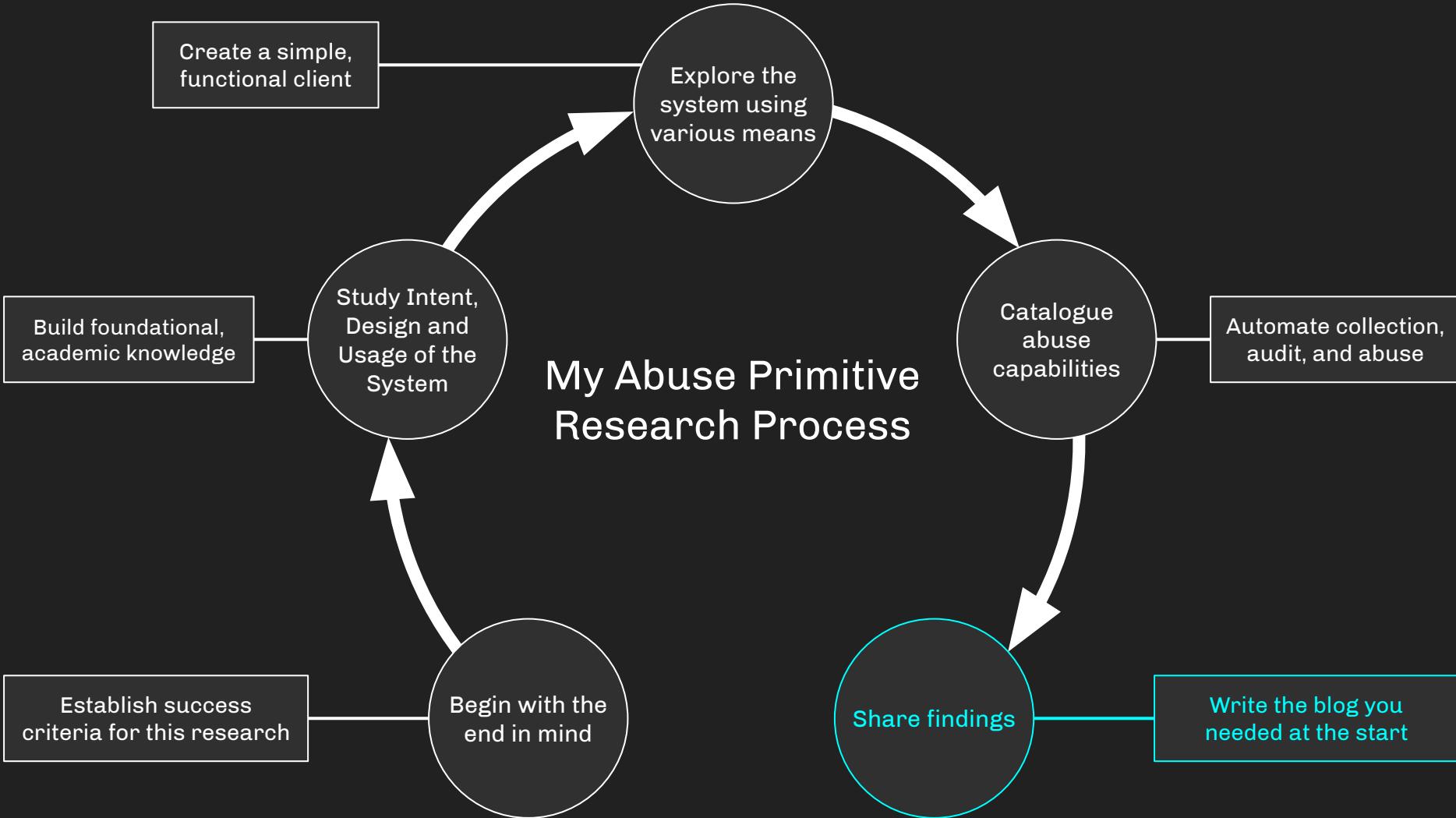
Share findings

Write a Blog

Share your
Code

Give a Talk

My Abuse Primitive Research Process





Begin with the
end in mind

I want to **understand**:

- The fundamental mechanics the system
- How the system interacts with other systems
- How the system can be abused

I want to **produce**:

- A blog/talk for others to understand and build on
- Example audit and abuse code
- Practical remediation guidance

If appropriate for **BloodHound**, I want to **prepare for**:

- The impact on the existing graph model
- How to expand the graph model
- What data to collect and ingest, and how to get that data



Begin with the
end in mind

I want to **understand**:

- The fundamental mechanics the system
- How the system interacts with other systems
- How the system can be abused

I want to **produce**:

- A blog/talk for others to understand and build on
- Example audit and abuse code
- Practical remediation guidance

If appropriate for **BloodHound**, I want to **prepare for**:

- The impact on the existing graph model
- How to expand the graph model
- What data to collect and ingest, and how to get that data

Agenda

Why Azure abuses?

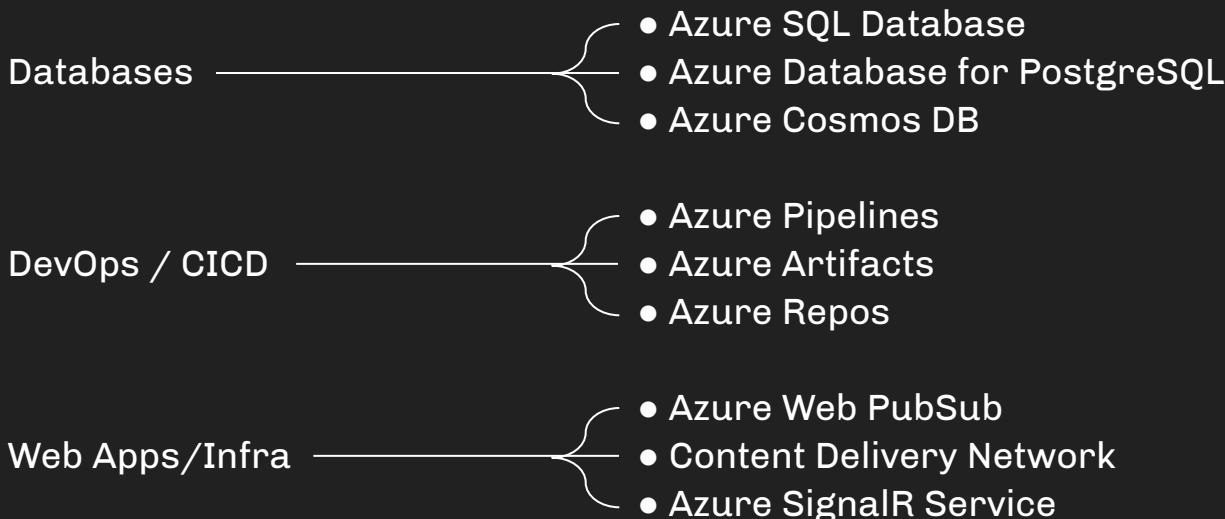
Crash Course Through The Basics

Finding New Attack Primitives: MS Graph Case Study

Where to find research ideas

Conclusion

Build on your existing expertise



See the full (?) directory of services here:

<https://azure.microsoft.com/en-us/services/>

Follow Microsoft Leaders on Twitter

@JefTek - Jef Kazimer

Principal Program Manager - Azure Active Directory

@BaileyBercick - Bailey Bercick

Program Manager - Azure Active Directory Product Group

@Sue_Bohn - Sue Bohn

Vice President of Program Management in the Identity & Network Access Division

@Alex_A_Simons - Alex Simons

Corporate Vice President of Program Management, Microsoft Identity Division

Follow These People on Twitter

[@mariussmellum](#) - Marius Solbakken

Principal - TietoEVRY

[@inversecos](#) - Lina Lau

Principal Incident Response Consultant - Secureworks

[@DrAzureAD](#) - Dr. Nestori Syynimaa

Senior Principal Security Researcher - Secureworks

[@asegunlolu](#) - David Okeyode

EMEA Chief Technology Officer, Azure Cloud - Palo Alto Networks

Bookmark these pages

<https://www.thelazyadministrator.com>

<https://goodworkaround.com/>

<https://www.azadvertiser.net/>

<https://thomasvanlaere.com/>

<https://msportals.io/?search=>

Agenda

Why abuses, not bugs?

Crash Course Through The Basics

Finding New Attack Primitives: MS Graph Case Study

Where to find research ideas

Conclusion

Conclusion

There has never been a better time than **right now** to get involved in Azure abuse research.

Conclusion

There has never been a better time than **right now** to get involved in Azure abuse research.

I hope I've shown you just how **easy** (if tedious) it actually is. Happy hunting!



SPECTEROPS

Thank you!

You can find me at [@ waldo](https://twitter.com/waldo)



Appendix Slides

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPldlJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet Saved to Drive

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

A1 MS Graph App Role Name

	A	B	C	D	E	F	G
1	MS Graph App Role Name						
2	-----						
3	AccessReview.Read.All						
4	AccessReview.ReadWrite.All						
5	AccessReview.ReadWrite.Membership						
6	AdministrativeUnit.Read.All						
7	AdministrativeUnit.ReadWrite.All						
8	Agreement.Read.All						
9	Agreement.ReadWrite.All						
10	AgreementAcceptance.Read.All						
11	APIConnectors.Read.All						
12	APIConnectors.ReadWrite.All						
13	AppCatalog.Read.All						
14	AppCatalog.ReadWrite.All						
15	Application.Read.All						
16	Application.ReadWrite.All						
17	Application.ReadWrite.OwnedBy						
18	AppRoleAssignment.ReadWrite.All						
19	AuditLog.Read.All						
20	BitlockerKey.Read.All						
21	BitlockerKey.ReadBasic.All						
22	Calendars.Read						
23	Calendars.ReadWrite						
24	CallRecord-PstrnCalls.Read.All						
25	CallRecords.Read.All						

+ Sheet1 >

```
49 # Try to grant "MyCoolApp" the "Global Admin" role:
50 $body = @{
51     "@odata.type" = "#microsoft.graph.unifiedRoleAssignment"
52     principalId = "d146464f-523a-4d24-bfce-17d21568647e"
53     roleDefinitionId = "62e90394-69f5-4237-9190-012177145e10"
54     directoryScopeId = "/"
55 }
56 $req = $null
57 $req = Invoke-RestMethod -Headers @{Authorization = "Bearer $($token.access_token)" } ` 
58     -Uri "https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments" ` 
59     -Method POST ` 
60     -Body $($body | ConvertTo-Json) ` 
61     -ContentType 'application/json'
62 $req
```

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPIdJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

C4

A B C D

	MS Graph App Role Name	Promote Self to Global Admin	Change Global Admin's Password	Add Principal to Role Enabled Se
1	MS Graph App Role Name			
2	-----			
3	AccessReview.Read.All	No	No	
4	AccessReview.ReadWrite.All			
5	AccessReview.ReadWrite.Membership			
6	AdministrativeUnit.Read.All			
7	AdministrativeUnit.ReadWrite.All			
8	Agreement.Read.All			
9	Agreement.ReadWrite.All			
10	AgreementAcceptance.Read.All			
11	APIConnectors.Read.All			
12	APIConnectors.ReadWrite.All			
13	AppCatalog.Read.All			
14	AppCatalog.ReadWrite.All			
15	Application.Read.All			
16	Application.ReadWrite.All			
17	Application.ReadWrite.OwnedBy			
18	AppRoleAssignment.ReadWrite.All			
19	AuditLog.Read.All			
20	BitlockerKey.Read.All			
21	BitlockerKey.ReadBasic.All			
22	Calendars.Read			
23	Calendars.ReadWrite			
24	CallRecord-PstrCalls.Read.All			
25	CallRecords.Read.All			

Sheet1

Explore

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPldlJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet Saved to Drive

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

D4

	A	B	C	D
1	MS Graph App Role Name	Promote Self to Global Admin	Change Global Admin's Password	Add Principal to Role Enabled Se
2	----			
3	AccessReview.Read.All	No	No	No
4	AccessReview.ReadWrite.All			
5	AccessReview.ReadWrite.Membership			
6	AdministrativeUnit.Read.All			
7	AdministrativeUnit.ReadWrite.All			
8	Agreement.Read.All			
9	Agreement.ReadWrite.All			
10	AgreementAcceptance.Read.All			
11	APIConnectors.Read.All			
12	APIConnectors.ReadWrite.All			
13	AppCatalog.Read.All			
14	AppCatalog.ReadWrite.All			
15	Application.Read.All			
16	Application.ReadWrite.All			
17	Application.ReadWrite.OwnedBy			
18	AppRoleAssignment.ReadWrite.All			
19	AuditLog.Read.All			
20	BitlockerKey.Read.All			
21	BitlockerKey.ReadBasic.All			
22	Calendars.Read			
23	Calendars.ReadWrite			
24	CallRecord-PstrCalls.Read.All			
25	CallRecords.Read.All			

Sheet1

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPIdJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet

File Edit View Insert Format Data Tools Help Last edit was seconds ago

D13

	A	B	C	D
1	MS Graph App Role Name	Promote Self to Global Admin	Change Global Admin's Password	Add Principal to Role Enabled Se
2	----			
3	AccessReview.Read.All	No	No	No
4	AccessReview.ReadWrite.All	No	No	No
5	AccessReview.ReadWrite.Membership	No	No	No
6	AdministrativeUnit.Read.All	No	No	No
7	AdministrativeUnit.ReadWrite.All	No	No	No
8	Agreement.Read.All	No	No	No
9	Agreement.ReadWrite.All	No	No	No
10	AgreementAcceptance.Read.All	No	No	No
11	APIConnectors.Read.All	No	No	No
12	APIConnectors.ReadWrite.All	No	No	No
13	AppCatalog.Read.All			
14	AppCatalog.ReadWrite.All			
15	Application.Read.All			
16	Application.ReadWrite.All			
17	Application.ReadWrite.OwnedBy			
18	AppRoleAssignment.ReadWrite.All			
19	AuditLog.Read.All			
20	BitlockerKey.Read.All			
21	BitlockerKey.ReadBasic.All			
22	Calendars.Read			
23	Calendars.ReadWrite			
24	CallRecord-PstrCalls.Read.All			
25	CallRecords.Read.All			

Sheet1

Explore

Untitled spreadsheet - Google Sheets

docs.google.com/spreadsheets/d/1UPIdlJpAYysf6wbC3ygBMCLw5ukOo-Q7G93KEE...

Untitled spreadsheet Saved to Drive

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

D24

	A	B	C	D
1	MS Graph App Role Name	Promote Self to Global Admin	Change Global Admin's Password	Add Principal to Role Enabled Se
2	----			
3	AccessReview.Read.All	No	No	No
4	AccessReview.ReadWrite.All	No	No	No
5	AccessReview.ReadWrite.Membership	No	No	No
6	AdministrativeUnit.Read.All	No	No	No
7	AdministrativeUnit.ReadWrite.All	No	No	No
8	Agreement.Read.All	No	No	No
9	Agreement.ReadWrite.All	No	No	No
10	AgreementAcceptance.Read.All	No	No	No
11	APIConnectors.Read.All	No	No	No
12	APIConnectors.ReadWrite.All	No	No	No
13	AppCatalog.Read.All	No	No	No
14	AppCatalog.ReadWrite.All	No	No	No
15	Application.Read.All	No	No	No
16	Application.ReadWrite.All	No	No	No
17	Application.ReadWrite.OwnedBy	No	No	No
18	AppRoleAssignment.ReadWrite.All	No	No	No
19	AuditLog.Read.All	No	No	No
20	BitlockerKey.Read.All	No	No	No
21	BitlockerKey.ReadBasic.All	No	No	No
22	Calendars.Read	No	No	No
23	Calendars.ReadWrite	No	No	No
24	CallRecord-PstrnCalls.Read.All			
25	CallRecords.Read.All			

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Is that app permission abusable?													
	Abuses												
	Groups				Service Principals / Apps				Directory Roles		App Roles		
Microsoft Graph API Permissions:	Add owner to role eligible group	Add member to role-eligible group	Add member to non-role eligible group	Add owner to non role-eligible group	Add secret to SP	Add owner to SP	Add secret to App Reg	Add Owner to App Reg	Promote a user to Global Admin		Grant an app role		
Application.ReadWrite.All	No	No	No	No	Yes	Yes	Yes	Yes	No		No		
AppRoleAssignment.ReadWrite.All	No	No	No	No	No	Yes	No	No	No		Yes		
DelegatedPermissionGrant.ReadWrite.All	No	No	No	No	No	No	No	No	No		No		
Directory.ReadWrite.All	No	No	Yes	Yes	No	No	No	No	No		No		
Group.ReadWrite.All	No	No	Yes	Yes	No	No	No	No	No		No		
GroupMember.ReadWrite.All	No	No	Yes	No	No	No	No	No	No		No		
RoleManagement.ReadWrite.Directory	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes		Yes		
ServicePrincipalEndpoint.ReadWrite.All	No	No	No	No	No	Yes	No	No	No		No		

Review: Catalogue the system's abuse capabilities

Actions:

- Determine the scope of objects that can be acted upon through the system
- For each object type, attempt to “abuse” the object through the system using various privileges
- Document your findings
- If possible, automate your abuse tests

Results:

- You should understand where the system materially differs from documentation
- You should now know at least some abuse primitives against the system
- You should now know what information to collect, and how, to find abusable configurations in the system
- You should be able to publish your findings for industry colleagues to understand and build on top of

Microsoft Azure

Search resources, services, and docs (G+)

arobbins@specterdev.o...
SPECTEROPS DEVELOPMENT (SP...)

Home > MyCoolApp

MyCoolApp | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest

Configure permissions

The "Admin consent required" column shows the default value for an organization. However, app will be used. [Learn more](#)

+ Add a permission ✓ Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description
Microsoft Graph (2)	Application	Manage app permission grants and application access
AppRoleAssignment.ReadWrite	Application	Manage app permission grants and application access
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try [Enterprise applications](#).

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services Allow validated users to read and write protected content

Azure Service Management Programmatic access to much of the functionality available through the Azure portal

Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM Access the capabilities of CRM business software and ERP systems

Flow Service Embed flow templates and manage flows

Request API permissions

Microsoft Graph

Azure Communication Services

Azure Key Vault

Azure Rights Management Services

Azure Service Management

Azure Storage

Dynamics 365 Business Central

Dynamics CRM

Flow Service

Red arrows point from the 'Grant admin consent for SpecterOps Development' button on the left to the 'Microsoft Graph' card on the right, and from the 'Microsoft Graph' card on the right to the 'Microsoft Graph' card in the 'Commonly used Microsoft APIs' section below it.

Microsoft Azure

Search resources, services, and docs (G+)

arobbins@specterdev.o...
SPECTEROPS DEVELOPMENT (SP...)

Home > MyCoolApp

MyCoolApp | API permissions

Search (Cmd+/) Refresh Got feedback?

Overview Quickstart Integration assistant

The "Admin consent required" column shows the default value for an organization. However, app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description
Microsoft Graph (2)		
AppRoleAssignment.ReadWrite.	Application	Manage app permission grants and ap...
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

All APIs Microsoft Graph https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Your application runs as a background service or daemon without a signed-in user.

Add permissions Discard



Microsoft Azure

Search resources, services, and docs (G+)

arobbins@specterdev.o...
SPECTEROPS DEVELOPMENT (SP...)

Home > MyCoolApp

MyCoolApp | API permissions

Search (Cmd+/) Refresh Got feedback?

The "Admin consent required" column shows the default value for an organization. However app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
AppRoleAssignment.ReadWrite	Application	Manage app permission grants and app roles	
User.Read	Delegated	Sign in and read user profile	

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

< All APIs

- > PrintJob
- > PrintSettings
- > PrintTaskDefinition
- > PrivilegedAccess (1)
 - PrivilegedAccess.Read.AzureAD ⓘ Read privileged access to Azure AD roles Yes
 - PrivilegedAccess.Read.AzureADGroup ⓘ Read privileged access to Azure AD groups Yes
 - PrivilegedAccess.Read.AzureResources ⓘ Read privileged access to Azure resources Yes
 - PrivilegedAccess.ReadWrite.AzureAD ⓘ Read and write privileged access to Azure AD roles Yes
 - PrivilegedAccess.ReadWrite.AzureADGroup ⓘ Read and write privileged access to Azure AD groups Yes
 - PrivilegedAccess.ReadWrite.AzureResources ⓘ Read and write privileged access to Azure resources Yes
- > ProgramControl
- > Reports

Add permissions Discard

Microsoft Azure

Search resources, services, and docs (G+)

Home > MyCoolApp

MyCoolApp | API permissions

Search (Cmd+/) Refresh Got feedback?

The "Admin consent required" column shows the default value for an organization. However app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description
Microsoft Graph (2)		
AppRoleAssignment.ReadWrite	Application	Manage app permission grants and applications
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try [Enterprise applications](#).

New Incognito Tab ⌘T

New Window ⌘N

New Incognito Window ⌘⌘N

Downloads ⌘⌘L

Bookmarks ⌘P

Zoom - 100% + ⌘P

Print... ⌘P

Cast... ⌘F

Find... ⌘F

More Tools ⌘P

Edit Cut Copy Paste ⌘C ⌘V ⌘X ⌘Z

Settings ⌘S

Help ⌘H

Save Page As... ⌘S

Create Shortcut... ⌘D

Name Window... ⌘W

Privileged Access Read Write Azure AD ⌘A

Clear Browsing Data... ⌘ShiftDelete

Extensions ⌘ShiftE

Task Manager ⌘ShiftT

Developer Tools ⌘ShiftI

PrivilegedAccess.ReadWrite.AzureADGroup ⌘A

PrivilegedAccess.ReadWrite.AzureResources ⌘A

Add permissions Discard

A red arrow points from the 'Developer Tools' option in the context menu towards the 'Add permissions' button at the bottom of the main page.

Microsoft Azure

Search resources, services, and docs (G+)

Home > MyCoolApp

MyCoolApp | API permissions

Refresh Got feedback?

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions is displayed below. Click Add permissions to grant additional permissions to your application.

Add permissions Discard

UserShiftPreferences

User

WindowsUpdates

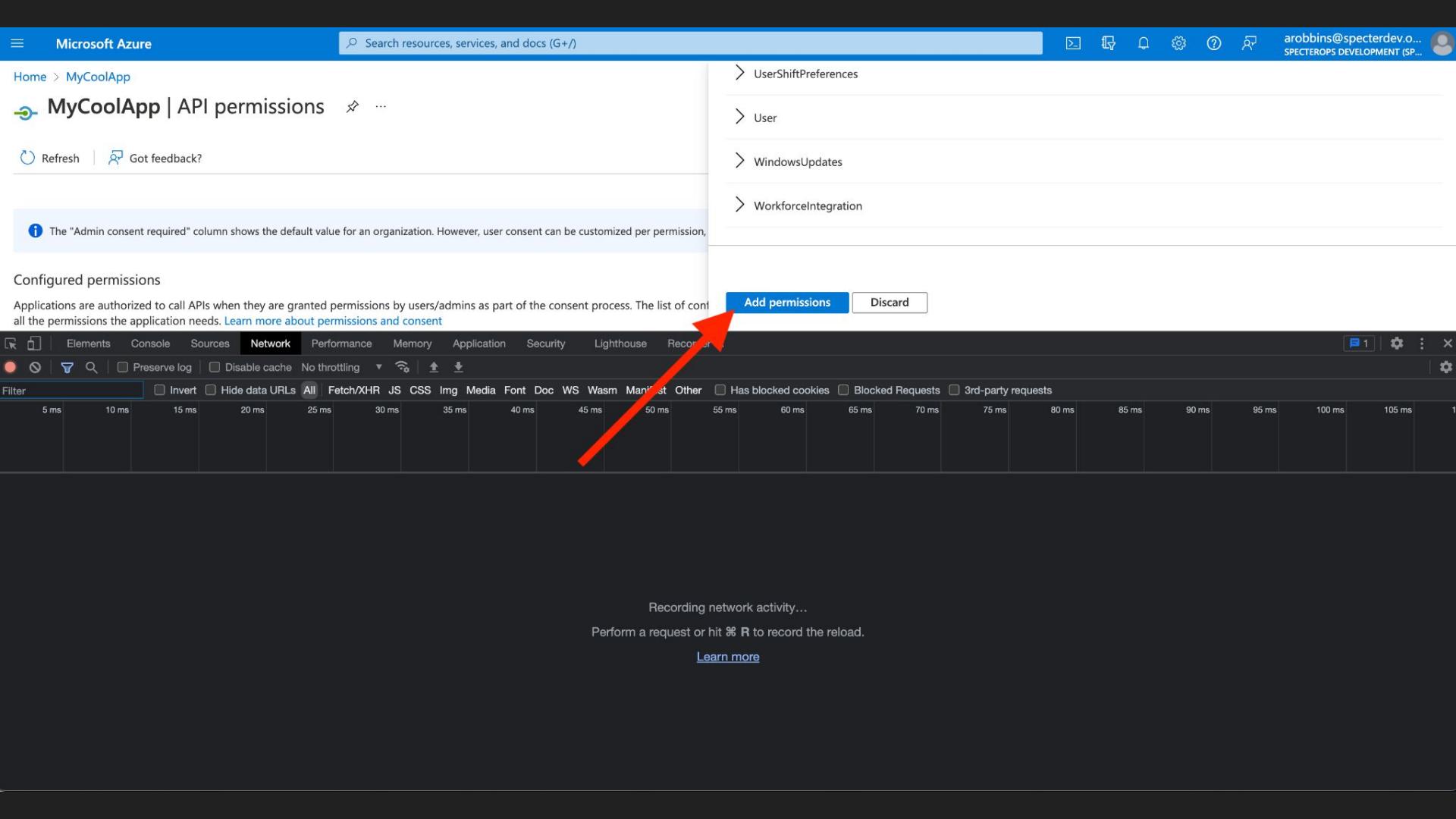
WorkforceIntegration

Network Performance Memory Application Security Lighthouse Recorder

Preserve log Disable cache No throttling

Filter Invert Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other Has blocked cookies Blocked Requests 3rd-party requests

Recording network activity...
Perform a request or hit ⌘ R to record the reload.
[Learn more](#)



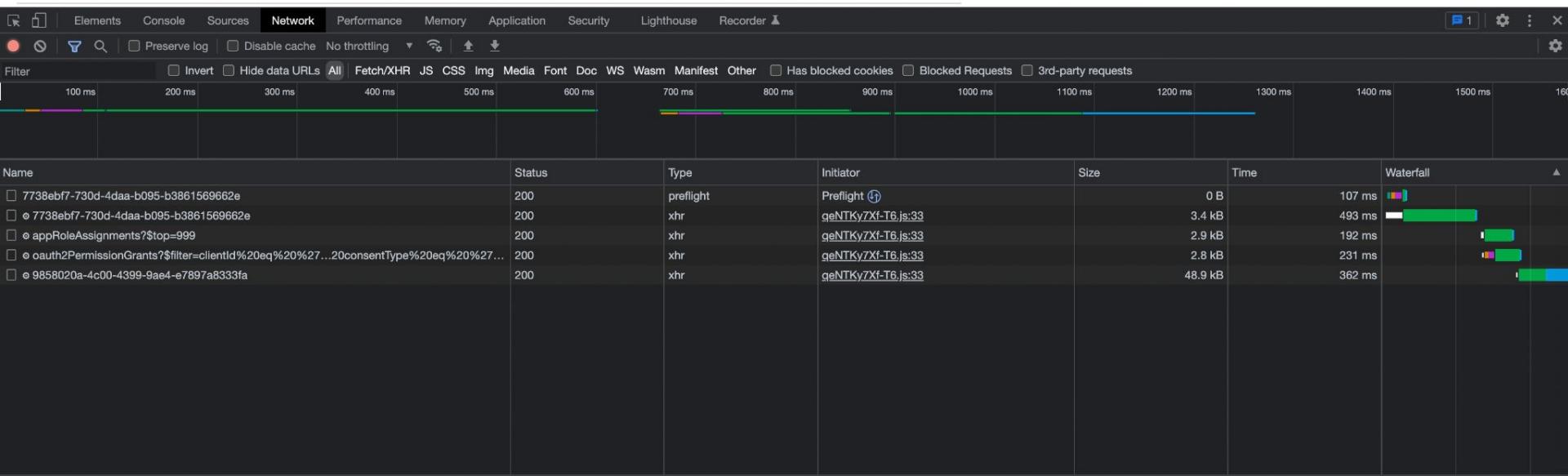
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description	Admin consent requ...	Status	...
▼ Microsoft Graph (3)					
AppRoleAssignment.ReadWrite.	Application	Manage app permission grants and app role assignments	Yes	✓ Granted for SpecterOps
PrivilegedAccess.ReadWrite.Azure	Application	Read and write privileged access to Azure AD roles	Yes	⚠ Not granted for Specter...	...



¹ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

 Add a permission Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				
AppRoleAssignment.ReadWrite.	Application	Manage app permission grants and app role assignments	Yes	✓ Granted for SpecterOps ...
PrivilegedAccess.ReadWrite.AzureAD	Application	Read and write privileged access to Azure AD roles	Yes	⚠ Not granted for Specter...

The screenshot shows the Network tab in the Chrome DevTools. A red arrow points from the 'Request Method' field in the General section to the 'PATCH' value. Another red arrow points from the 'Status Code' field to the '200 OK' value. The 'Request URL' is https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e.

Request URL: https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e

Request Method: PATCH

Status Code: 200 OK

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

 Add a permission  Grant admin consent for SpecterOps Development

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				
AppRoleAssignment.ReadWrite.	Application	Manage app permission grants and app role assignments	Yes	✓ Granted for SpecterOps ...
PrivilegedAccess.ReadWrite.Azure	Application	Read and write privileged access to Azure AD roles	Yes	⚠ Not granted for Specter...

The screenshot shows the Network tab in Google Chrome DevTools. A context menu is open over a specific network request. The menu includes options like 'Open in new tab', 'Copy link address', 'Copy response', 'Copy stack trace', 'Copy as PowerShell', 'Copy as fetch', 'Copy as Node.js fetch', and 'Copy as cURL'. The 'Copy as cURL' option is highlighted with a red arrow. The URL for the request is also visible in the menu.

The screenshot shows the Postman application interface. At the top, there is a navigation bar with icons for Home, Workspaces, API Network, Reports, and Explore. To the right of the navigation bar is a search bar labeled "Search Postman". Further to the right are icons for Cloud, Invite, Notifications, Settings, and Upgrade.

The main area displays a collection named "Office365" under the "Collections" section. Within this collection, there is a folder named "Azure Research". The "Azure Research" folder is currently selected, indicated by a blue border around its title bar. The title bar also contains buttons for "New", "Import", and "X".

The "Azure Research" folder contains the following sections:

- Authorization**: This tab is currently active, showing the message: "This authorization method will be used for every request in this collection. You can override this by specifying one in the request."
- Pre-request Script**
- Tests**
- Variables**

Below the tabs, there is a "Type" dropdown menu set to "No Auth". A note below the tabs states: "This collection does not use any authorization. [Learn more about authorization](#)".

On the far right of the interface, there are several status indicators and links: "Share" (with a red dot), "Fork" (with a count of 0), "Run" (with a count of 0), "Save" (with a count of 0), "Watch" (with a count of 0), and a "More" link.

The left sidebar lists other workspace categories: APIs, Environments, Mock Servers, Monitors, Flows, and History.

At the bottom of the screen, there are navigation links for "Find and Replace", "Console", "Capture requests and cookies", "Bootcamp", "Runner", "Trash", and a help icon.



Home

Workspaces

API Network

Reports Explore

Search Postman



Invite



Upgrade

Office365

New Import

Azure Research X

+

...

No Environment

...

Collections



Azure Research

This collection is empty
[Add a request](#) to start working

APIs

Environments

Mock Servers

Monitors

Flows

History

Azure Research

Share

Fork

0

Run

Save

Watch

0

...

Import

[File](#) [Folder](#) [Link](#) [Raw text](#) [Code repository](#) [New](#)[OpenAPI](#) [GraphQL](#) [cURL](#)[WSDL](#) [NEW](#) [HAR](#) [NEW](#)

OR

Upload Files

[Learn more](#) about the different import formats supported



Home

Workspaces

API Network

Reports Explore

Search Postman



Invite



Upgrade



Office365

New Import

Azure Research

+ ...

No Environment



Collections



APIs



Environments



Mock Servers



Monitors



Flows



History

Azure Research

Share

Fork

0

Run

Save

Watch

0



Import

[File](#) [Folder](#) [Link](#) [Raw text](#) [Code repository](#) [New](#)

Paste raw text

```
p.g. curl --location --request GET "https://postman-echo.com/get"
```



Continue



Find and Replace

Console

Capture requests and cookies

Bootcamp

Runner

Trash





Home

Workspaces

API Network

Reports Explore

Search Postman



Invite



Upgrade



Office365

New Import

Azure Research

+ ...

No Environment



Collections



Azure Research

This collection is empty
Add a request to start working



APIs

Environments

Mock Servers

Monitors

Flows

History

Import

Select files to import · 1/1 selected

NAME	FORMAT	IMPORT AS
https://graph.microsoft.com/v1.0/myorganiz...	Curl	Request



Cancel

Import



Find and Replace



Console

Capture requests and cookies

Bootcamp

Runner

Trash





Office365

New Import

Azure Research

PATCH https://graph.mi... ● + ⋮

No Environment



Collections



Azure Research

APIs

This collection is empty
Add a request to start working.

Environments

Mock Servers

Monitors

Flows

History

https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e

Save ⋮



Send ⋮

Cookies

PATCH https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e

Params

Authorization

Headers (21)

Body

Pre-request Script

Tests

Settings

Query Params

KEY	VALUE	DESCRIPTION	⋮	Bulk Edit
Key	Value	Description		

Response



Click Send to get a response



Find and Replace



Console

Capture requests and cookies

Bootcamp

Runner

Trash





Home

Workspaces

API Network

Reports Explore

Search Postman



Invite



Upgrade



Office365

New Import

Azure Research

PATCH https://graph.mi...

+

...

No Environment



Collections



Azure Research

APIs

Environments

Mock Servers

Monitors

Flows

History

https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e

Save



Send



PATCH https://graph.microsoft.com/v1.0/myorganization/applications/7738ebf7-730d-4daa-b095-b3861569662e

Cookies

Params

Authorization

Headers

(21)

Body

Pre-request Script

Tests

Settings

Beautify

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1  {"requiredResourceAccess": [{"resourceAppId": "00000003-0000-0000-c000-000000000000", "resourceAccess": [ { "id": "e1fe6dd8-ba31-4d61-88e7-88639da4683d", "type": "Scope"}, {"id": "06b708a9-e830-4db3-a914-8e69da51d44f", "type": "Role"}, {"id": "854d9ab1-6657-4ec8-be45-823027bcd009", "type": "Role"}]}]
```

Body Cookies Headers (13) Test Results

Status: 200 OK Time: 317 ms Size: 3.77 KB

Save Response



Pretty

Raw

Preview Visualize

JSON



```
1  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#applications/$entity",
2  "id": "7738ebf7-730d-4daa-b095-b3861569662e",
3  "deletedDateTime": null,
4  "appId": "4a2d703b-ec39-4fe4-98a9-e298d5a0f540",
5  "applicationTemplateId": null,
6  "disabledByMicrosoftStatus": null,
7  "createdDateTime": "2021-11-30T20:31:46Z",
8  "displayName": "MyCoolApp",
9  "description": null,
10 "groupMembershipClaims": null,
11 "identifierUris": [],
12 "isDeviceOnlyAuthSupported": null,
13 "isFallbackPublicClient": null,
```



Find and Replace



Console

Capture requests and cookies

Bootcamp

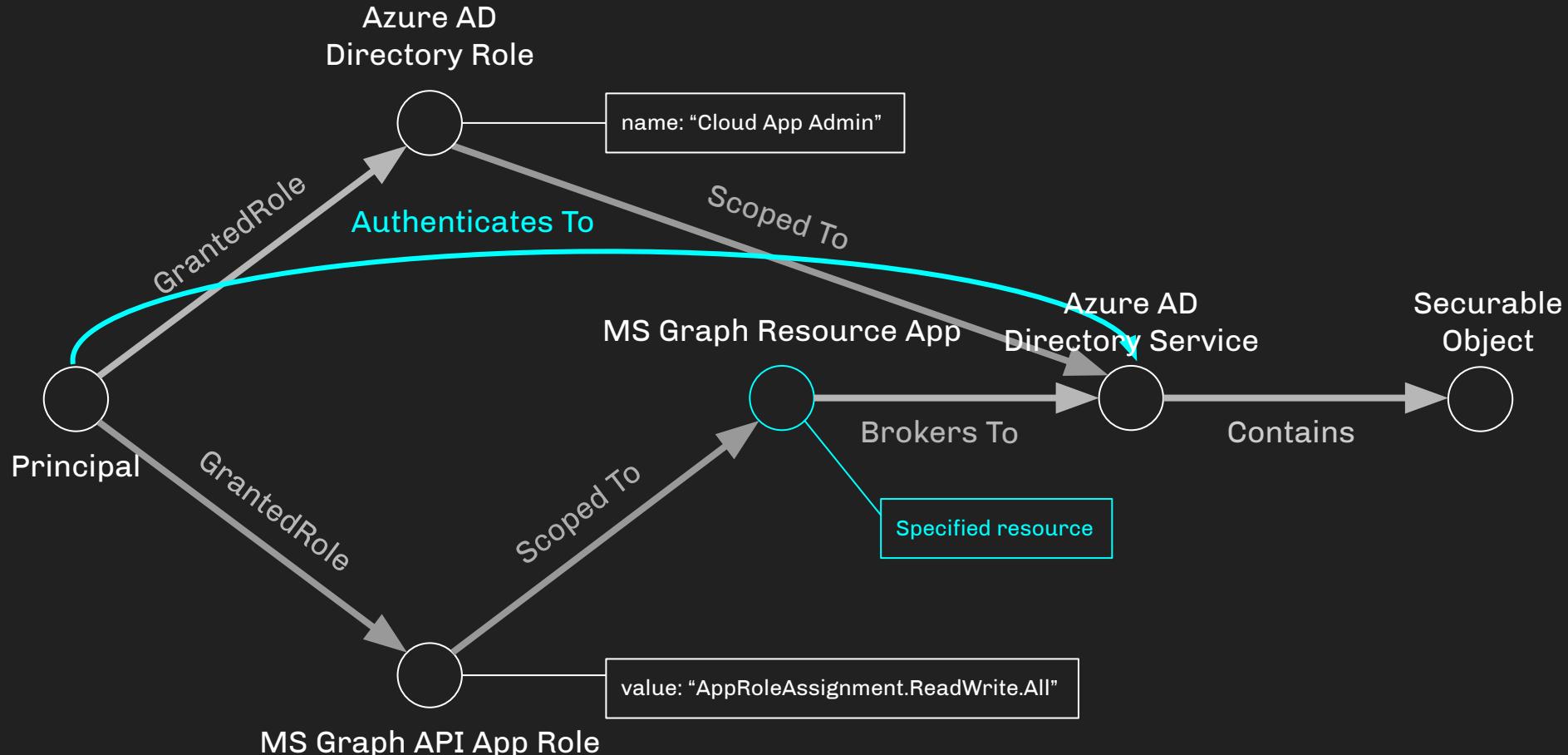
Runner

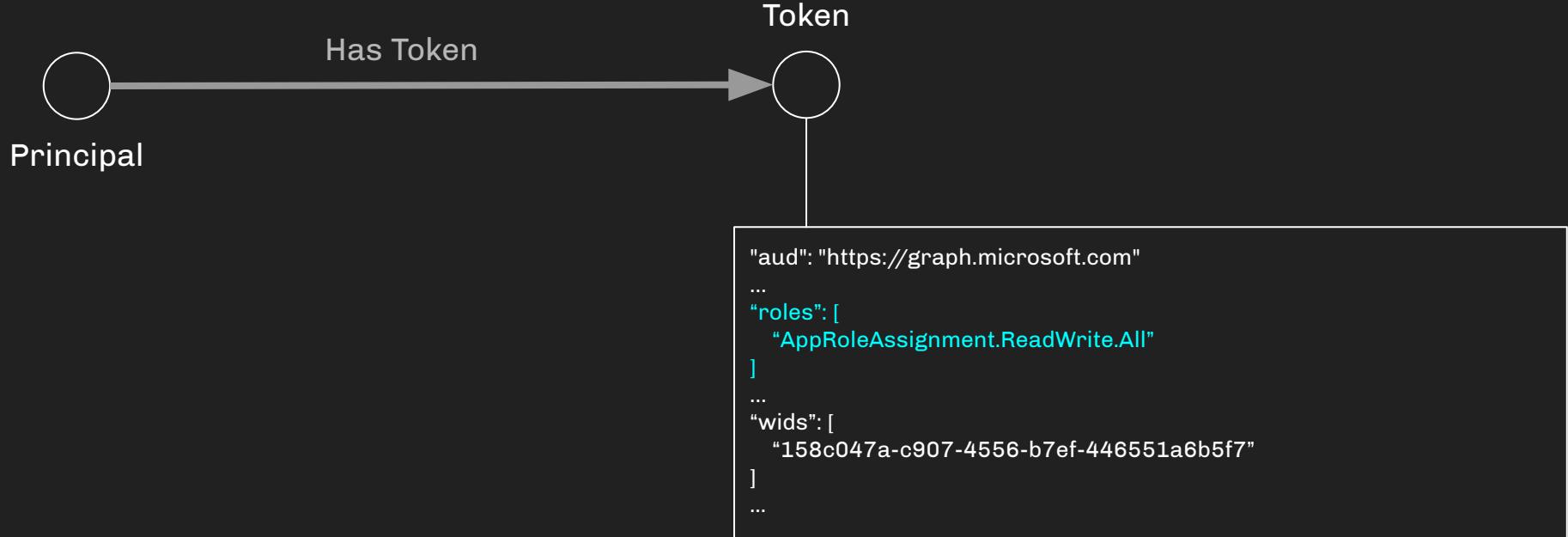
Trash



Fine-grained control lets you:

- Determine the minimum parameters actually required by the API
- Easily change request properties to test for CA bypasses
- Accurately automate your testing
- Build future tooling without needing 3rd party modules
- Discover how the system materially differs from its documentation
- VASTLY simplify getting data out of the system
- Get MORE data than what the GUI will ever show you





```
PS C:\Users\andyrobbins> # Now that we have a bearer token, we can interface with the MS Graph API
PS C:\Users\andyrobbins> $URI      = 'https://graph.microsoft.com/v1.0/Groups/'
PS C:\Users\andyrobbins> $Request   = Invoke-RestMethod ` 
>>           -Headers @{Authorization = "Bearer $($token.access_token)"} ` 
>>           -URI $URI ` 
>>           -Method GET
PS C:\Users\andyrobbins> $Request.value | Select -First 1

id                      : 0b57a21e-4fe0-4bb7-a7a8-4764bcc1b3bf
deletedDateTime          :
classification           :
createdDateTime          : 2021-11-03T22:33:56Z
creationOptions          : {}
description              :
displayName              : AAD DC Administrators
expirationDateTime       :
groupTypes               : {}
isAssignableToRole       :
mail                     :
mailEnabled              : False
mailNickname             : AADDCAAdministrators
membershipRule           :
membershipRuleProcessingState :
onPremisesDomainName    :
onPremisesLastSyncDateTime :
onPremisesNetBiosName   :
onPremisesSamAccountName :
onPremisesSecurityIdentifier :
onPremisesSyncEnabled    :
preferredDataLocation    :
preferredLanguage         :
proxyAddresses           : {}
renewedDateTime           : 2021-11-03T22:33:56Z
resourceBehaviorOptions  : {}
resourceProvisioningOptions :
securityEnabled           : True
securityIdentifier        : S-1-12-1-190292510-1270304736-1682417831-3216228796
theme                    :
visibility               :
onPremisesProvisioningErrors : {}
```

My High Level Methodology:

1. Begin with the end in mind
2. Understand the intent and design of the system
3. Explore the system from different perspectives
4. Catalogue the system's abuse capabilities